Supravegherea serviciilor de informații

Set de instrumente

Editat de Hans Born și Aidan Wills





DCAF
a centre for security, development and the rule of law



Ministry of Foreign Affairs of the Netherlands

Supravegherea serviciilor de informații

Set de instrumente

Editat de Hans Born și Aidan Wills



Supravegherea serviciilor de informații

Set de instrumente

Editat de Hans Born și Aidan Wills

Centrul pentru controlul democratic al forțelor armate (DCAF) de la Geneva este o fundație internațională cu misiunea de a sprijini comunitatea internațională în realizarea bunei guvernanțe și reformarea sectorului de securitate. Centrul dezvoltă și promovează norme și standarde, realizează cercetări tematice individualizate, identifică bune practici și recomandări pentru promovarea guvernanței democratice în sectorul de securitate și asigură sprijin consultativ la nivel de țară, precum și programe de asistență cu caracter practic.

Publicat de DCAF, Geneva
11 Rue de Chantepoulet
Geneva – 1201
Elveția
www.dcaf.ch

Designer: Alice Lake-Hammond, www.alicelakehammond.com
Fotografie copertă: Hans Kouwenhoven

Traducere în română: Cristina Sever și Cristina Dumitrescu

Realizarea acestei publicaţii a fost posibilă cu sprijinul generos al Ministerului Afacerilor Externe din Olanda

ISBN: 978-92-9222-222-2

CUPRINS

CUVÂNT ÎNAINTE AL DCAF

Domeniul intelligence reprezintă o ultimă frontieră în procesele de democratizare și reformare a sectorului de securitate. Așa cum au demonstrat multe democrații consolidate, guvernanţa democratică și statul de drept ajung în sfera intelligence multă vreme după ce au dobândit baze solide în alte domenii ale statului. În multe democrații consolidate, înființarea sistemelor de supraveghere a serviciilor de informații a urmat o traiectorie comună: anumite activități ale serviciilor de informații au generat îngrijorare în privința încălcării proceselor democratice legitime și în raport cu exercitarea drepturilor omului și a libertăților fundamentale, ceea ce a dus la o perioadă de studiu și cercetare psihologică și la crearea, ca rezultat, a unor noi mecanisme de supraveghere.

Democrațiile emergente nu au nevoie să recurgă la această abordare reactivă. „Tranziția" le oferă o prețioasă oportunitate de a pune baze solide, legale și instituționale, pentru activitatea de supraveghere a serviciilor de informații. Totuși, trebuie să fim conștienți că stabilirea acestor baze nu e decât un mic pas în procesul interminabil și dificil prin care trebuie să ne asigurăm că serviciile sunt eficace în protejarea securității naționale, a siguranței publice și a drepturilor omului, dar, în același timp, respectă statul de drept și practica democratică. Îndeplinirea pe termen lung a acestor obiective reclamă interes, vigilență și dedicare continue din partea celor implicați în supraveghere, precum și un efort asiduu de evaluare şi îmbunătăţire a sistemelor de supraveghere. Am încredere că acest set de instrumente poate servi ca resursă importantă în sprijinul unei astfel de activităţi.

Parlamentarilor le revine o mare responsabilitate atât în dezvoltarea cadrului legal și instituțional al activității de supraveghere, cât și pentru a se asigura, în calitate de principali supraveghetori externi, că supravegherea își atinge obiectivele sus-menționate. În acest domeniu, mai mult decât în oricare altul, parlamentarii trebuie să se străduiască să-și subordoneze interesele de partid unui scop mai important, acela de a proteja ordinea democratică și constituțională. Însă nu numai parlamentarii sunt cei cărora ar trebui să le revină toate responsabilitățile supravegherii externe – adeseori, le lipsesc timpul, experiența și independența necesare. Având în vedere acest lucru, ei trebuie să apeleze la organisme independente de supraveghere cu statut legal, precum instituțiile supreme de audit, instituțiile de tip

ombudsman și organismele specializate de supraveghere, invitându-le să joace un rol central în sfera lor de competență.

Deşi există multe publicații referitoare la supravegherea serviciilor de informații, majoritatea acestora se axează pe cadrul legal și instituțional al organismelor de supraveghere. Prezentul set de instrumente porneşte de la această abordare, explicând decidenților multe din provocările și dificultățile care apar pe parcursul conceperii, modificării și consolidării unui sistem de supraveghere. Însă, autorii contributori se aventurează dincolo de întrebările legate de conceperea acestor sisteme, oferind orientări practice, clare privind modul în care supraveghetorii externi pot aborda provocarea de a examina cu minuţiozitate aspecte specifice din munca serviciilor de informații. Sper ca lucrarea de față să poată contribui, de asemenea, la sensibilizarea societății civile și a mass-mediei cu privire la importanţa pe care o au diferitele aspecte ale supravegherii serviciilor de informații, și sper ca aceste grupuri să poată utiliza cunoştinţele dobândite pentru a-i trage la răspundere pe parlamentari şi pe alţi supraveghetori independenţi în legătură cu exercitarea controlului asupra serviciilor de informaţii sau cu lipsa acestuia.

Setul de instrumente se va bucura, probabil, de cel mai mare interes din partea decidenților implicaţi în dezvoltarea sistemelor de supraveghere a serviciilor de informații, a membrilor și staffului din organismele de supraveghere recent înființate, precum și a unor organizații ale societății civile. Cu toate că cei interesați pot fi în majoritate din state în tranziție, nu trebuie ignorată valoarea analizei făcute de autori pentru cei implicați – direct sau indirect – în supravegherea serviciilor de informații în democraţiile consolidate. În fapt, am ferma convingere că acest set de instrumente oferă exemple și argumente care vor provoca discuții despre posibila extindere sau întărire a controlului în aceste state.

De mai bine de 10 ani, DCAF sprijină eforturile de consolidare a capacității de supraveghere a serviciilor de informații nu numai în democrațiile emergente, dar și în sistemele democratice mai bine consolidate. DCAF consideră că reforma sistemelor de supraveghere a serviciilor de informații este o parte integrantă a proceselor de reformare a sectorului de securitate în contextul tranziției. În vreme ce unii donatori alocă un volum substanțial de resurse pentru îmbunătățirea capacității operaționale a serviciilor de informații din statele în tranziție (în vederea pregătirii unor parteneri operaționali eficienți), o importanță crucială revine investiţiei făcute atât de statele donatoare, cât și de statele beneficiare în dezvoltarea și menținerea

unor sisteme de supraveghere durabile și eficace. Sper ca acest set de instrumente să poată contribui la redresarea echilibrului între eficacitatea operațională și guvernanță prin conștientizarea, la nivelul comunităţii implicate în reformarea sectorului de securitate, a faptului că supravegherea serviciilor de informații este absolut necesară.

Ambasador Theodor H. Winkler
Director, DCAF

CUVÂNT ÎNAINTE

În copilărie, eram fascinat de caleidoscoape și mai sunt și acum, ca adult. Tot ce ții în mâini e un mic tub care are la un capăt un capac din sticlă mată, iar la celălalt, o mică gaură rotundă. Dacă scuturi cu grijă tubul, auzi de obicei un ușor clinchet. Dar nu-ți imaginezi ce este înăuntrul lui.

Când privești prin micul orificiu, nu vezi nimic dacă nu ții tubul în așa fel, încât lumina să străbată prin sticla mată. Doar atunci descoperi brusc un mozaic complex. Și, răsucind tubul, vei vedea cum se schimbă modelul mozaicului. E fascinant!

Într-un fel, această carte arată oarecum ca un caleidoscop. În fond, lumea intelligence este o cutie neagră pe care trebuie să o manevrezi într-un mod anume pentru a reuși să înțelegi ce se află înăuntru. Mai mult, perspectiva pare să se schimbe continuu.

Totuși, ceea ce vede un observator mai atent merită întotdeauna atenţie şi este, în același timp, interesant în măsura în care privitorul va dori să împărtășească celorlalți ceea ce a înțeles. Fapt care nu e atât de simplu cum ar părea, deoarece tainele tubului ce conține lumea intelligence nu pot fi dezvăluite pur și simplu.

Cartea de față intenționează să pună la dispoziție un ansamblu de instrumente ce permit organismelor de supraveghere să țină tubul îndreptat corect spre lumină și să prezinte ulterior ceea ce au observat, într-o manieră bine fundamentată.

În elaborarea acestor instrumente, autorii au evidenţiat diverse aspecte ale supravegherii, așezând diferite sisteme de supraveghere unul lângă altul și creând astfel o imagine caleidoscopică, ce confirmă faptul că există mai mult de un singur tip de supraveghere, invitându-ne să privim încontinuu la minunata lume a muncii de informații dintr-o perspectivă nouă şi critică.

În consecință, nu numai cei interesați din afara domeniului, dar, cu siguranță, și cei din interiorul lui – organismele de supraveghere și cele supuse supravegherii – vor profita de pe urma studierii acestei cărți.

Bert van Delden
Președinte, Comisia olandeză de Verificare a Serviciilor de Informații și de Securitate

MULȚUMIRI

Editorii doresc să-și exprime recunoștința față de Ministerul Afacerilor Externe din Olanda, al cărui generos sprijin a făcut posibilă realizarea acestei lucrări. Îndeosebi, dorim să mulțumim următorilor membri ai Departamentului pentru Politica de Securitate și Apărare pentru sprijinul și cooperarea lor neprețuite pe parcursul alcătuirii lucrării: Jacco Bos, Hein Knegt, Michael Stibbe, Frank van Beuningen și Joep Wijnands.

De asemenea, dorim să ne exprimăm gratitudinea față de Comisia olandeză de Verificare a Serviciilor de Informații și de Securitate (CTIVD) și, în special, faţă de preşedintele ei, Bert van Delden, fostul secretar al comisiei, Nick Verhoeven și actualul secretar al acesteia, Hilde Bos-Ollerman. CTIVD a asigurat un sprijin esențial în inițierea acestui proiect, iar comisia și-a oferit cu generozitate expertiza pe parcursul realizării lucrării. Totodată, editorii doresc să adreseze mulțumiri fostului ministru olandez al apărării și senator Wim van Eekelen, al cărui sprijin s-a dovedit indispensabil pentru DCAF și pentru reușita acestui proiect.

Totodată, editorii rămân îndatorați față de Agincourt Press, al cărui staff a răspuns de corectarea şi editarea variantei finale a textului pentru cea mai mare parte a lucrării. Stafful de la Agincourt Press a lucrat neobosit pentru a asigura consecvența limbajului și a stilului, precum și, pe cât posibil, un caracter accesibil al lucrării pentru cititorul fără expertiză în materie. Dorim să mulțumim în același timp și lui Alice Lake-Hammond pentru excelenta ei muncă de design și pentru înaltul profesionalism cu care a realizat punerea în pagină şi tehnoredactarea lucrării.

În final, dorim să mulțumim fostului nostru coleg, Gabriel Geisler Mesevage, care a fost coautor al instrumentului introductiv și, în plus, a avut și o contribuție semnificativă la conceperea și alcătuirea lucrării.

Hans Born și Aidan Wills
Geneva, iulie 2012

INSTRUMENTUL 1

Introducere în supravegherea serviciilor de informații

Hans Born și Gabriel Geisler Mesevage



1
Introducere în supravegherea serviciilor de informații

Hans Born și Gabriel Geisler Mesevage

1. INTRODUCERE

Instrumentul de față prezintă cititorului subiectul supravegherii serviciilor de informații, punându-i la dispoziție răspunsuri concise la întrebările fundamentale cine, ce, când, cum și de ce. Totodată, prezintă cititorilor celelalte instrumente din această lucrare, referitoare la supravegherea serviciilor de informații, instrumente care, în ansamblu, oferă răspunsuri mai elaborate atât la întrebările de mai sus, cât și la alte întrebări.

Scopul acestui proiect este de a reuni câțiva dintre cei mai remarcabili experți din domeniul supravegherii serviciilor de informații, care să-și prezinte cunoștințele într-o formă inteligibilă pentru cei fără expertiză în materie. Lucrarea își propune să îi ajute pe cititori să înțeleagă mai bine problemele relevante și să le ofere mai multe perspective comparative celor cu responsabilități în sfera supravegherii.

Acest instrument introductiv începe cu o privire generală asupra procesului de supraveghere a serviciilor de informații, incluzând descrierea instituțiilor implicate și a „ciclului de supraveghere a serviciilor de informații." În continuare, se explică motivul pentru care supravegherea în domeniul intelligence este importantă pentru apărarea drepturilor omului și a libertăților fundamentale ale indivizilor, precum și pentru creşterea siguranței lor. Sunt studiate apoi standardele și practicile actuale în supravegherea serviciilor de informații, punându-se accentul pe ceea ce majoritatea experților consideră a fi bune practici. Capitolul se încheie cu recomandări pentru întărirea supravegherii serviciilor de informații.

1.1 DE CE UN SET DE INSTRUMENTE PENTRU SUPRAVEGHEREA SERVICIILOR DE INFORMAȚII?

Acest set de instrumente a fost creat pentru a ajuta democrațiile emergente să înființeze servicii civile de supraveghere a serviciilor de informații, iar democrațiile consolidate – să le amelioreze. Lucrarea are patru obiective principale:

1. să ofere o orientare pertinentă din punct de vedere al politicilor în domeniu cu privire la crearea și consolidarea unor noi sisteme de supraveghere, precum și la revizuirea și ameliorarea celor existente.
2. să ofere indicații privind supravegherea unor aspecte specifice ale activităților serviciilor de informații, inclusiv culegerea de informații, utilizarea datelor cu caracter personal și schimbul de informații.
3. să determine o conștientizare, în rândul societății civile și al mass-mediei, cu privire la importanța pe care o are supravegherea serviciilor informațiilor.
4. să promoveze transferul de cunoștințe și de norme între țări, prin identificarea și analizarea diferitelor abordări, standarde și practici în domeniul supravegherii serviciilor de informații.

Prin urmare, în acest set de instrumente, nu se pune accentul pe o analiză academică abstractă, ci pe prezentarea unor îndrumări practice pentru cei care supraveghează serviciile de informații și/sau interacționează în mod regulat cu sistemele de supraveghere. Din acest motiv am ales să folosim formatul setului de instrumente, care se axează pe exemple practice și pe recomandări specifice, reflectând practici din întreaga lume.

1.2 TEME ABORDATE ÎN SETUL DE INSTRUMENTE

Cele nouă instrumente din lucrare constituie prezentări de sine stătătoare ale unor teme importante referitoare la supravegherea serviciilor de informații (a se vedea Tabelul 1). Fiecare din ele a fost redactat astfel, încât să poată fi citit în mod individual.

1.3 CUI SE ADRESEAZĂ LUCRAREA ?

Lucrarea a fost gândită în primul rând pentru cei care sunt implicaţi, direct sau indirect, în supravegherea serviciilor de informații. O astfel de audienţă include membri ai puterilor executivă, legislativă şi judecătorească și stafful lor, oficiali din domeniul intelligence, membri ai societății civile și ai mass-mediei.

Avem încredere că lucrarea se va bucura de un larg interes public. Totodată, există anumite sfere în care conținutul lucrării va fi considerat deosebit de util.

TABELUL 1: PREZENTARE GENERALĂ A INSTRUMENTELOR		
Instrumentul	**Titlul**	**Principalele întrebări abordate**
1	Introducere în supravegherea serviciilor de informații	• Ce este supravegherea serviciilor de informații • De ce e importantă supravegherea serviciilor de informații? • Care sunt responsabilitățile diferitelor instituții implicate în supravegherea serviciilor de informații?
2	Înființarea unor sisteme eficace de supraveghere a serviciilor de informații	• Care sunt avantajele și dezavantajele diferitelor abordări instituționale în supravegherea serviciilor de informații? • Care sunt obstacolele în calea unei supravegheri eficace și cum pot fi abordate? • Care sunt principalele considerente în conceperea cadrului legal și instituțional pentru supravegherea serviciilor de informații?
3	Transparența, secretizarea și supravegherea în domeniul intelligence într-o democrație	• Care este echilibrul corect între secretizare și transparență pentru serviciile de informații într-o democrație? • Ce poate fi considerată bună practică în privința legislației referitoare la protecția informațiilor și accesul la informaţii? • Care sunt nevoile de informare ale parlamentului, ale organismelor specializate de supraveghere și ale publicului, în domeniul intelligence ?
4	Efectuarea supravegherii	• Care sunt tipurile de abordare și metodele folosite de organismele de supraveghere pentru a trage la răspundere serviciile de informații? • Cum pot organismele de supraveghere să investigheze în mod eficace practicile serviciilor de informații? • Cum pot organismele de supraveghere să raporteze despre investigațiile lor?
5	Supravegherea culegerii de informații	• De ce e importantă supravegherea procesului de culegere a informațiilor? • Cum pot organismele de supraveghere să monitorizeze în mod eficace procesul de culegere a informațiilor? • Care sunt obstacolele în calea unei supravegheri eficace a procesului de culegere a informațiilor și cum pot fi abordate?

6	Supravegherea utilizării datelor cu caracter personal	• De ce e importantă supravegherea utilizării datelor cu caracter personal? • Cum pot organismele de supraveghere să se asigure că serviciile de informații utilizează datele cu caracter personal numai cu deplina respectare a legii ? • Care sunt obstacolele în calea unei supravegheri eficace a utilizării datelor cu caracter personal și cum pot fi abordate?
7	Supravegherea schimbului de informații	• De ce este importantă supravegherea schimbului de informații? • Care e rolul pe care ar trebui să îl joace organismele de supraveghere în privința schimbului de informații? • Care sunt obstacolele în calea unei supravegheri eficace a schimbului de informații pe plan intern și internațional și cum pot fi depăşite?
8	Supravegherea financiară a serviciilor de informații	• De ce este importantă supravegherea finanțelor de care dispun serviciile de informații? • De ce este nevoie pentru ca serviciile de informații să răspundă din punct de vedere financiar? • Care sunt rolul și responsabilitățile diferitelor instituții implicate în supravegherea financiară a serviciilor de informații?
9	Gestionarea reclamațiilor privind serviciile de informații	• De ce sunt importante mecanismele de gestionare a reclamațiilor? • Ce tipuri de sisteme de gestionare a reclamațiilor există? • Cum pot fi ameliorate sistemele de gestionare a reclamațiilor?

De exemplu, deoarece, instrumentele examinează îndeaproape rolul organismelor parlamentare și specializate de supraveghere, membri și angajați ai acestor instituții vor considera informațiile din lucrare ca având o relevanță deosebită. Similar, ziariști și membri ai societății civile, al căror domeniu de activitate include analiza serviciilor de informații, vor descoperi multe lucruri utile în lucrare, la fel ca şi oficialii guvernamentali implicaţi actualmente în crearea sau reformarea sistemelor de supraveghere a serviciilor de informații.

2. CE ESTE SUPRAVEGHEREA SERVICIILOR DE INFORMAȚII?

Această secțiune evidenţiază sfera de acțiune și contextul în care are loc supravegherea serviciilor de informații și aduce în discuţie instituţiile implicate. Din motive de concizie și claritate, lucrarea folosește termenul generic de „serviciu de informații" pentru a face referire la entități denumite în diverse feluri: „servicii de securitate," „servicii/organizații pentru informații de securitate" și „agenții de informații."[1] Deoarece diferitele jurisdicții structurează activitatea de intelligence în diferite moduri, acest set de instrumente folosește o abordare funcțională pentru definirea *serviciului de informații*. Concret, el definește un serviciu de informații ca o organizație de stat, care culege, analizează și diseminează informații legate de amenințări la adresa securității naționale.

O asemenea definiție acoperă o gamă largă de organizații – incluzând serviciile de informații militare, ale poliţiei şi civile, atât interne, cât și din străinătate. Totodată, definiţia include organizații adeseori trecute cu vederea, care funcționează frecvent în cadrul ministerelor de finanțe și al departamentelor de trezorerie, așa cum sunt agențiile care au sarcina de a investiga finanțarea terorismului sau de a preveni spălarea banilor. După cum relatează *Manualul privind reforma sectorului de securitate*, publicat de Comisia de Asistenţă pentru Dezvoltare a OCDE, „Cele mai multe țări au o multitudine de organizații de informații, cu responsabilități distincte, care se suprapun uneori. Acestea includ agenții de informații interne și externe, de informații tactice și strategice, de informații în domeniul criminalității, agenții de culegere a datelor (de exemplu, comunicații, informații din surse umane și date de tip imagine, agenții de informații civile și militare și organisme de evaluare strategică."[2] Împreună, aceste agenții alcătuiesc „comunitatea de informații."

Serviciile de informații se diferențiază față de alte agenții guvernamentale și datorită competențelor speciale de care dispun în culegerea de informații – așa cum sunt competența de a intercepta comunicații, competența de a opera o supraveghere sub acoperire, competența de a utiliza informatori secreți și competența de a intra clandestin în locuințe. În unele state (precum Danemarca, Malaysia, Rusia și Suedia), serviciile de informații au și puteri

[1] Acest set de instrumente folosește termenul de *serviciu de informații* mai curând decât pe cel de *agenție de informații* sau *organism de informații* pentru a sublinia faptul că asemenea organizații îndeplinesc un serviciu public.

[2] Organizația pentru Cooperare și Dezvoltare Economică, *OECD DAC Handbook on Security System Reform: Supporting Security and Justice* [*Manualul OECD DAC privind reforma sistemelor de securitate: sprijinirea securității și justiției*] (Paris, OECD, 2007), p. 140.

polițienești și, de aceea, sunt numite uneori „servicii de securitate ale poliției" sau „sectoare speciale." În alte state, activitatea serviciilor de poliție este complet separată de activitatea serviciilor de informații: acestea din urmă nu dispun de puteri polițienești (de exemplu, să aresteze, să rețină și să interogheze suspecți).

Deși definiția pe care am folosit-o restrânge aria serviciilor de informații la organizații ale statului, există anumite țări în care guvernul utilizează contractori privați pentru a desfășura muncă de informații.[3] Deoarece supravegherea activității contractorilor privați diferă substanțial de supravegherea activității serviciilor publice, ea nu este analizată în lucrarea de față.

2.1 SFERA DE CUPRINDERE A SUPRAVEGHERII SERVICIILOR DE INFORMAȚII

Supravegherea este un termen atotcuprinzător, care înglobează examinarea *ex ante*, monitorizarea pe parcurs și verificarea ex post, precum și evaluarea și investigarea. Ea este efectuată de conducerea superioară a serviciilor de informații, de oficiali ai executivului, membri ai puterii judecătorești și parlamentari, de instituții independente de tip ombudsman, de instituții de audit, organisme specializate de supraveghere, ziariști și membri ai societății civile.

Supravegherea trebuie diferențiată de *control* deoarece ultimul termen (ca și managementul) implică prerogativa de a orienta politicile și activitățile unei organizații. Astfel, *controlul* e asociat, de regulă, cu ramura executivă a guvernului, și anume cu conducerea superioară a serviciilor de informații. Un exemplu de control, în opoziție cu supravegherea, ar fi emiterea unui ordin prin care se cere unui serviciu de informații să adopte o nouă prioritate, cum ar fi lupta împotriva terorismului. Cititorii trebuie să fie totuși conștienți că nu orice guvern face o distincție clară între supraveghere și control. Este motivul pentru care unele instituții descrise în acest set de instrumente ca fiind organisme de supraveghere pot avea, totodată, o serie de responsabilități de control.

Scopul principal al supravegherii este de a trage la răspundere serviciile de informații pentru politicile și acțiunile lor din punct de vedere al legalității, corectitudinii, eficacității și eficienței acestora.[4] Procesul prin care un organism de supraveghere trage la răspundere un serviciu de informații are, de obicei, trei faze distincte:

---

[3] Pentru informații privind contractorii privați, a se vedea Tim Shorrock, *Spies for Hire: The Secret World of Intelligence Outsourcing* [*Spioni de închiriat: lumea secretă a externalizării serviciilor de informații*] (New York: Simon & Schuster, 2008).

[4] Pentru o discuție mai amplă asupra a ceea ce înseamnă a trage la răspundere o agenție publică, a se vedea Mark Bovens, *Public Accountability* [*Responsabilitatea publică*] în *The Oxford Handbook of Public Management*, editori Ewan Ferlie, Laurence E. Lynne Jr, și Christopher Pollitt (Oxford: Oxford University Press, 2005).

1. Organismul de supraveghere culege informații despre serviciul de informații.
2. Pe baza acestor informații inițiale, organismul de supraveghere începe un dialog cu serviciul de informații.
3. Organismul de supraveghere face cunoscute constatările și recomandările sale.

Astfel, pentru a funcționa în mod eficace, un organism de supraveghere trebuie să aibă capacitatea de a accede la informațiile relevante, de a adresa întrebări oficialilor din domeniul intelligence și de a face cunoscute constatările și recomandările sale în baza celor aflate. Fără aceste trei competențe, nu poate exista o responsabilitate reală, și, probabil, procesul de supraveghere a serviciilor de informații va eșua.

Supravegherea se poate referi nu numai la corectitudinea și legalitatea activităților unui serviciu, dar și la eficacitatea și eficiența lui. În acest context, *corectitudinea* se referă la existența unei justificări morale a acțiunilor serviciului de informații, în vreme ce *legalitatea* se referă la existența conformității acestor acțiuni cu legea care le guvernează. *Eficacitatea* măsoară gradul în care un serviciu își atinge obiectivele, în vreme ce *eficiența* măsoară economicitatea cu care un serviciu își urmărește obiectivele. În unele state, organismele de supraveghere a serviciilor de informații se ocupă exclusiv de legalitate (de exemplu, Comisia olandeză de Verificare a Serviciilor de Informații și de Securitate); în alte state, legea mandatează organismele de supraveghere să se concentreze exclusiv asupra eficacității și eficienței (de exemplu, Comisia pentru informații și securitate din Marea Britanie).

2.2 RESPONSABILITĂȚI INSTITUȚIONALE

O supraveghere eficace a serviciilor de informații necesită nu numai o activitate coordonată a diferitelor organisme de stat, ci și examinarea activă a conduitei structurilor guvernamentale de către membri ai societății civile și ai mass-mediei. Deși toate aceste organisme au roluri importante, lucrarea de față își concentrează atenția în primul rând asupra organismelor parlamentare și specializate de supraveghere, deoarece acestea nu răspund nici în fața serviciilor de informații, nici a executivului, ceea ce înseamnă că sunt mai bine plasate pentru a apăra în mod independent responsabilitatea democratică și respectul pentru statul de drept și drepturile omului.

Tabelul 2 oferă o privire de ansamblu asupra responsabilităților asumate, în general, de organisme publice și private în procesul de supraveghere. Cititorii ar trebui, totuși, să observe că responsabilitățile respective sunt abordate diferit de la țară la țară și că sistemul de supraveghere al unui anumit stat poate să nu includă toate responsabilitățile menționate în tabel.

TABELUL 2: ORGANISMELE DE SUPRAVEGHERE ȘI PRINCIPALELE LOR RESPONSABILITĂȚI	
Organisme de supraveghere	**Responsabilități principale**
Conducerea superioară a serviciilor de informații	• Implementează controalele interne și monitorizează conformarea • Dezvoltă o cultură instituţională care promovează respectul față de statul de drept și drepturile omului • Analizează cererile de utilizare a puterilor speciale și transmite solicitări organismelor externe pentru acordarea permisiunii necesare • Asigură cooperarea cu organismele interne și externe de supraveghere • Aplică regulile care interzic ordinele ilegale și acordă sprijin funcționarilor care refuză să se supună acelor ordine • Implementează şi monitorizează procedurile de protecţie a informatorilor interni
Executivul	• Numeşte conducerea superioară a serviciilor de informații • Stabileşte politicile şi priorităţile serviciilor de informații și emite liniile directoare • Prezintă în parlament rapoarte privind activitățile serviciilor de informații • Asigură coperarea serviciilor de informații cu alte organisme de supraveghere în domeniul intelligence • Stabileşte bugetele serviciilor de informații și examinează cheltuielile acestora • Aprobă cooperarea dintre serviciile de informații și alte servicii și agenții, atât interne, cât și străine • Autorizează cererile de utilizare a puterilor speciale • Aprobă operaţiunile sensibile ale serviciilor de informații
Organismele de supraveghere parlamentare și specializate	• Adoptă şi amendează un cadru legal cuprinzător privind serviciile de informații și supravegherea acestora • Evaluează corectitudinea, legalitatea, eficacitatea şi eficienţa activităților desfășurate de serviciile de informații • Aprobă și verifică bugetele serviciilor de informații
Puterea judecătorească	• Autorizează *ex ante* și/sau verifică *ex post* modul de utilizare a puterilor speciale de către serviciile de informații • Judecă cazurile de drept penal, civil, constituțional și administrativ, care se referă la activitățile serviciilor de informații • Participă (în calitate personală) ca membri în organisme specializate de supraveghere, precum și la anchete *ad hoc* independente.
Instituțiile de tip ombudsman	• Examinează reclamaţiile împotriva serviciilor de informații • Inițiază investigații tematice privind activitatea serviciilor de informații

Instituțiile supreme de audit	• Evidențiază problemele legate de legalitate, eficiență și eficacitate în managementul financiar și formulează recomandări pentru îmbunătățirea managementului financiar • Asigură parlamentul în privința exactității și ritmicității bilanțurilor contabile ale guvernului, contribuind astfel la asigurarea faptului că executivul respectă voinţa parlamentului • Asigură populația că banii publici sunt cheltuiți în mod legal, adecvat, eficient și eficace
Societatea civilă și mass-media	• Investighează politicile şi activităţile serviciilor de informații și ale organismelor de supraveghere a acestora • Expune conduita incorectă, ilegală, ineficace sau ineficientă a serviciilor de informații • Informează opinia publică despre politicile și activitățile serviciilor de informații și despre activitatea de supraveghere a acestora • Încurajează dezbaterea publică pe tema politicilor și activităților serviciilor de informații, precum și despre munca organismelor de supraveghere a serviciilor de informații

2.2.1 Conducerea superioară a serviciilor de informații

O supraveghere eficace în domeniul intelligence începe prin controale interne eficace. Oficialii din executiv, comisiile parlamentare și organismele specializate, toate vor întâmpina dificultăți în îndeplinirea responsabilităților lor de supraveghere în situația în care conducerea superioară a unui serviciu de informații este delăsătoare și/sau nu cooperează. Pe de altă parte, în cazul în care conducerea superioară se implică și își oferă sprijinul, controalele interne ale serviciilor și sistemele de management pot oferi protecție împotriva abuzului de putere și a încălcării drepturilor omului.

Implementarea controalelor interne și monitorizarea conformării

Conducerea superioară poartă direct răspunderea pentru dezvoltarea controalelor interne și conformarea cu acestea – controale pe care Comisia de la Veneția le definește ca „structuri de decizie, al căror rol este să se asigure că măsurile și politicile sunt autorizate corespunzător”.[5] Altfel spus, controalele interne îi fac răspunzători pe ofițerii de informații pentru conduita lor în cadrul mandatului legal al serviciului, în raport cu prioritățile definite pentru serviciul respectiv de către executiv și cu politicile și reglementările stabilite de condu-

[5] Consiliul Europei, Comisia Europeană pentru Democrație prin Drept (Comisia de la Veneția), *Report on the democratic oversight of the security services* [*Raport privind controlul democratic al serviciilor de securitate*], CDL-AD(2007)016 (2007), Paragraful 73.

cerea superioară a serviciului. Controalele interne includ și proceduri pentru realizarea, în mod corespunzător, a bugetării și evidenței documentelor.

Dezvoltarea unei culturi instituționale care promovează respectul față de statul de drept și drepturile omului

Necesitatea ca serviciile de informații să dezvolte și să mențină culturi instituționale care respectă statul de drept și drepturile omului este recunoscută pe scară largă.[6] Legile și reglementările care promovează asemenea culturi sunt, deci, importante, dar nu suficiente. Conducerea superioară a serviciilor trebuie, la rândul ei, să dezvolte și să pună în practică programe concepute pentru a induce angajaților o înțelegere a ceea ce înseamnă constituționalitatea, legalitatea, responsabilitatea și integritatea.

Analizarea cererilor de utilizare a puterilor speciale și transmiterea solicitărilor către organisme externe pentru acordarea permisiunii necesare

În majoritatea statelor, utilizarea puterilor speciale de către un serviciu de informații este supusă, în ultimă instanță, aprobării ministeriale și/sau celei judecătorești, datorită impactului pe care asemenea puteri îl pot avea asupra drepturilor omului. Cu toate acestea, conducerea superioară a unui serviciu are un rol foarte important în selectarea cererilor care merită să fie transmise acestor organisme externe. Conducerea trebuie să ia asemenea decizii analizând gradul de intruziune a operațiunii respective în raport cu natura amenințării. Riscurile mai mari la adresa drepturilor omului ar trebui să impună o autorizare internă de la niveluri mai înalte.

Asigurarea cooperării cu organismele interne și externe de supraveghere

Conducerea superioară a serviciului este responsabilă pentru funcționarea eficace a tuturor organismelor interne de supraveghere. Responsabilitatea în cauză include asigurarea faptului că angajații serviciului cooperează deplin cu organismele interne de supraveghere, precum și cu organismele externe de supraveghere. În plus, conducerea superioară trebuie să izoleze organismele de supraveghere (în particular, cele interne) împotriva presiunilor administrative, astfel încât acestea să poată funcționa efectiv ca mecanisme de gestionare a reclamațiilor.

---

[6] Ca exemplu, a se vedea Ronnie Kasrils, „To spy or not to spy? Intelligence and democracy in South Africa” [„A spiona sau a nu spiona? Intelligence și democrație în Africa de Sud”], în *To spy or not to spy? Intelligence and democracy in South Africa*, ed. Lauren Hutton (Pretoria: Institute for Security Studies, 2009), pp. 9–20.

Aplicarea regulilor care interzic ordinele ilegale și sprijinirea ofițerilor care refuză să se supună acestor ordine

Conducerea superioară trebuie să întreprindă toate acțiunile necesare pentru a se asigura că nu se dau ordine ilegale; și că, dacă sunt date, ele nu sunt respectate. Atare demers se poate fundamenta pe legi de protejare a informatorilor interni, care permit personalului unui serviciu de informații să dezvăluie organismelor interne ori externe desemnate informații ce denotă un comportament incorect. În unele state, au fost create proceduri legale în scopul raportării unei activități discutabile din domeniul intelligence către directorul serviciului de informații sau către un alt oficial mandatat în acest scop. În Bosnia și Herțegovina, o activitate discutabilă este raportată inspectorului general al serviciului respectiv (a se vedea Caseta 1). În alte țări, este raportată ministrului responsabil.[7] În plus, legile naționale din unele state (precum Bulgaria [8]) prevăd că angajații serviciului de informații sunt trași la răspundere în mod individual pentru acțiuni ilegale și/sau pentru încălcarea obligațiilor lor oficiale.

Caseta 1: Obligația ofițerilor de informații de a raporta o activitate ilegală în Bosnia și Herțegovina

În cazul în care un angajat consideră că a primit un ordin ilegal, acesta/aceasta va aduce la cunoștința celui care a emis ordinul îngrijorarea sa cu privire la ilegalitatea lui. Dacă cel care a dat ordinul îl repetă, angajatul va cere o confirmare scrisă a unui astfel de ordin. În situația în care angajatul continuă să aibă rezerve, el/ea va înainta ordinul persoanei imediat superioare celei care l-a emis și va raporta cazul Inspectorului General. Angajatul poate refuza să îl ducă la îndeplinire.[9]

2.2.2 Executivul

Doctrina responsabilității ministeriale [10] prevede că fiecare ministru răspunde în fața șefului statului, a cabinetului și a parlamentului, pentru modul în care își

7 Ca exemplu, a se vedea SUA, Departamentul Apărării, „Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO))" [„Asistentul Secretarului Apărării pentru supravegherea serviciilor de informații (ATSD(IO))"], Directiva Nr. 5148.11, 21 mai 2004.

8 Bulgaria, *Law on State Agency for National Security* [*Lege privind Agenția de Stat pentru Securitate Națională*], a 40-a Sesiune a Adunării Naționale, Articolul 88.

9 Bosnia și Herțegovina, *Law on the Intelligence and Security Agency* [*Lege privind Agenția de Informații și Securitate*], 22 martie 2004, Articolul 42.

10 Africa de Sud, Comisia ministerială de verificare a serviciilor de informații, *Intelligence in a Constitutional Democracy: Final Report to the Minister for Intelligence Services, the Honourable Mr. Ronnie Kasrils, MP* [*Intelligence într-o democrație*

exercită puterile și funcțiile.[11] În temeiul acestei doctrine, executivul, care stabilește politicile serviciilor de informații, este răspunzător din punct de vedere politic pentru conduita acestora.

De regulă, serviciile de informații raportează unui ministru din guvern, însărcinat să asigure funcționarea corectă, legală, eficace și eficientă a serviciului respectiv. În Germania, de exemplu, serviciile de informații externe, interne și militare raportează șefului Cancelariei Federale și, respectiv, ministrului de interne și ministrului apărării.[12]

Nivelul controlului exercitat de executiv variază de la un stat la altul. Complexitatea muncii de informații poate face dificile monitorizarea și controlul de către executiv a conduitei serviciilor. Într-adevăr, „în practică, monopolul cunoștințelor de specialitate, deținut de agenție,” după cum a remarcat Comisia de la Veneția, „va garanta prin el însuși agenției un grad de autonomie considerabil față de controlul guvernamental.”[13]

Deși oficialii din executiv sunt interesați în cea mai mare măsură să evite eșecurile din domeniul intelligence, ei nu manifestă un interes la fel de mare pentru dezvăluirea eșecurilor atunci când acestea se produc. Dezvăluirea publică a unor întâmplări nedorite sau a unor fapte reprobabile poate stânjeni din punct de vedere politic și poate afecta negativ cariera miniștrilor implicați. Din acest motiv, unii experți nu au încredere în capacitatea executivului de a efectua o supraveghere corectă a serviciilor de informații, bazându-se, în schimb, pe examinarea și criticarea de către parlament, puterea judecătorească și societatea civilă a deciziilor luate de guvern.

În pofida acestei îngrijorări, executivul constituie o verigă importantă în lanțul responsabilităților. Aceste responsabilități, enumerate în Tabelul 2, arată clar că, pe lângă responsabilitățile politice, executivul are și responsabilități

---

constituțională: Raport final în atenția ministrului pentru serviciile de informații, *Hon. Mr. Ronnie Kasrils, MP*] (10 septembrie 2008), p. 77.

[11] În Olanda, responsabilitatea ministerială a fost statuată în Constituție chiar din 1848; a se vedea A.D. Belinfante, *Beginselen van Nederlands Staatsrecht* [*Principiile dreptului constituțional olandez*] (Alphen aan de Rijn: Samson Publishers, 1981), pp. 64–66.

[12] Christian Heyer, „Parliamentary Oversight of Intelligence: The German Approach” [„Supravegherea parlamentară a serviciilor de informații: abordarea germană”], în *Intelligence and Human Rights in the Era of Global Terrorism*, ed. Steve Tsang (Westport, CT: Praeger Security International, 2007), p. 69.

[13] Consiliul Europei, Comisia Europeană pentru Democrație prin Drept (Comisia de la Veneția), *Report on the democratic oversight of the security services* [*Raport privind controlul democratic al serviciilor de securitate*], CDL-AD(2007)016 (2007), Paragraful 78.

operaționale legate de serviciile de informații, în special în privința implementării politicilor. De aceea, este important ca informațiile referitoare la decizii operaționale dificile ori sensibile să nu fie ascunse celor din executiv. Dimpotrivă, executivul trebuie informat întotdeauna.

2.2.3 Organismele parlamentare și specializate de supraveghere

Instituirea și menținerea, de către executiv, a unei supravegheri eficace a activităților din domeniul informațiilor de securitate este esențială, la fel ca și existența unei supravegheri independente, atât parlamentare, cât și neparlamentare. Caracterul secret al muncii în domeniul intelligence, lipsa expunerii ei la examinare și interpretare judiciare, amenințarea la adresa drepturilor omului pe care o reprezintă urmărirea excesivă a persoanelor, precum și existenţa unor greșeli anterioare, toate subliniază necesitatea unei supravegheri efective a serviciilor de informații de către organisme independente în raport cu guvernul în funcție.[14]

În general, comisiile parlamentare de supraveghere și organismele specializate asigură cea mai eficace supraveghere externă. Cele dintâi pot fi împărțite, din rațiuni practice, în două categorii: comisii generale cu mandate ample (cum sunt comisiile de apărare și de afaceri externe) și comisii specializate, care se ocupă exclusiv de comunitatea de informații. Deși comisiile generale (îndeosebi din sfera bugetului și finanțelor) pot avea anumite responsabilități de supraveghere în privința serviciilor de informații, cea mai mare parte a activităților de supraveghere în domeniul intelligence se desfășoară, de regulă, de către comisii specializate, datorită faptului că membrii acestora au mai multă experiență și expertiză și pentru că o astfel de abordare limitează cercul de cunoștințe și informații la membrii comisiilor și nu îl extinde la ansamblul parlamentarilor.

Organismele specializate de supraveghere a serviciilor de informații (denumite uneori „instituții specializate de supraveghere” sau „organisme specializate neparlamentare de supraveghere”) sunt înființate și funcționează independent față de executiv, parlament și serviciile de informații pe care sunt mandatate să le supravegheze. Organismele specializate de supraveghere au și ele avantajul unor membri cu expertiză și al unui obiect de activitate bine delimitat. În majoritatea statelor, asemenea organisme dispun de experți în domeniul intelligence, care pot fi foști sau actuali judecători, procurori și șefi ai serviciilor

[14] Comisia de anchetă privind activitățile Poliției Călare Regale Canadiene (Comisia McDonald), *First Report: Security and Information* [*Primul raport: securitate și informații*] (9 octombrie, 1979), p. 425.

de poliție.[15] Într-adevăr, membrii organismelor specializate de supraveghere au adesea o experiență și o expertiză mai mari în comparație cu membrii comisiilor parlamentare specializate. În plus, membrii organismelor specializate au, de obicei, libertatea de a se dedica în întregime supravegherii serviciilor de informații, în vreme ce parlamentarii fac parte din mai multe comisii și, în consecință, trebuie să facă față mai multor responsabilități. Un alt avantaj al organismelor specializate de supraveghere este acela că membrii lor nu sunt nici politicieni de profesie și nici nu sunt direct implicați în activitatea politică de zi cu zi, astfel încât conduita lor tinde să fie mult mai puțin politizată decât aceea a parlamentarilor. Totuși, organismele specializate ar trebui să fie totdeauna văzute ca o completare a supravegherii parlamentare și nu ca un substitut al ei, deoarece principiile guvernanței democratice impun controlul direct al parlamentului asupra tuturor activităților guvernului.

Unele state (precum Australia, a se vedea Caseta 2) au întărit supravegherea serviciilor de informații prin desemnarea unui inspector general independent. Denumirea, mandatul, competențele și atribuțiile acestei funcții variază considerabil de la un stat la altul (a se vedea Farson – Instrumentul 2), dar misiunile ei de bază includ, de regulă, urmărirea respectării de către serviciile de informații a constituției, a legilor proprii de funcționare și a politicilor operaționale stabilite de executiv. Alte funcții comune includ:

- instruirea personalului serviciilor de informații cu privire la drepturile și responsabilitățile lui;
- efectuarea auditului și a inspecțiilor interne – în special în vederea depistării și prevenirii risipei, fraudei și abuzului;
- asigurarea menținerii unor politici și proceduri eficace de securitate;
- primirea și investigarea reclamațiilor făcute de personalul serviciilor;
- asigurarea difuzării informațiilor pe care publicul este îndreptățit să le primească în virtutea legislației referitoare la libertatea de informare;
- asigurarea de către serviciu a evidenței documentelor conform legislației și politicilor relevante.[16]

Mandatele comisiilor parlamentare de supraveghere și ale organismelor specializate de supraveghere variază de la un stat la altul. Unele țări (precum SUA, prin comisiile din Congres însărcinate cu supravegherea serviciilor de informații) au adoptat mandate care acoperă întregul spectru privind corecti-

[15] Unele state utilizează o formă hibridă de organism de supraveghere, ai cărui membri includ atât experți independenți, cât și foști parlamentari.

[16] A se vedea Marea Britanie, Comisia pentru informații și securitate, *Annual Report 2001–2002*, CM 5542 [*Raportul anual 2001–2002*, CM 5542] (2002), pp. 46–50.

Caseta 2: Inspectorul General australian pentru informații și securitate

Inspectorul General australian (IG) pentru informații și securitate oferă primului ministru, miniștrilor de rang superior și parlamentului o asigurare independentă că serviciile de informații ale țării și alte agenții de securitate acționează legal și corect. IG oferă această asigurare prin investigarea serviciilor de informații și a agențiilor de securitate și prezentarea de rapoarte cu privire la activitățile lor. Mandatul Inspectorului General mai include sarcina de a urmări dacă operațiunile serviciilor de informații și ale agențiilor de securitate sunt eficace și manifestă respect față de drepturile omului.

Pentru îndeplinirea mandatului său, IG e împuternicit de legea australiană să întreprindă anchete la cererea ministrului responsabil sau din proprie inițiativă. În plus, este împuternicit să primească și să investigheze reclamațiile făcute de persoanele lezate de activitatea serviciilor de informații. Asemenea investigații pot include inspecția în incinte ale serviciilor de informații (așa cum sunt locurile de detenție), luarea unei mărturii sub jurământ și accesul la documente. La încheierea fiecărei anchete, IG înaintează ministrului responsabil un raport al cărui rezumat este, de obicei, inclus în raportul anual pe care îl prezintă parlamentului australian. Directorul serviciului în cauză și ministrul responsabil sunt obligați prin lege să raporteze IG implementarea oricăreia din recomandările conținute în raportul său.[17]

tudinea, legalitatea, eficacitatea și eficiența; alte țări (precum Olanda și Suedia) limitează mandatele unor astfel de organisme numai la legalitate.

Pentru îndeplinirea acestor mandate, comisiilor parlamentare de supraveghere și organismelor specializate de supraveghere li se acordă adeseori competențe largi, ce pot include oricare din – sau chiar toate – puterile din lista de mai jos (care nu e exhaustivă):

- accesarea informațiilor clasificate;
- primirea și verificarea rapoartelor anuale și a altor rapoarte elaborate de serviciile de informații;
- citarea unor oficiali din executiv și din domeniul intelligence, pentru a depune mărturie sub jurământ;
- invitarea unor experți externi și a altor persoane pentru a depune mărturie sub jurământ;

[17] Pentru informații mai detaliate, a se vedea Australia, Inspector-General of Intelligence and Security Act 1986, Act No. 101 of 1986 as amended [Lege privind Inspectorul General pentru informații și securitate din 1986, Legea nr. 101 din 1986 amendată]; și web site-ul Inspectorului General pentru informații și securitate (disponibil la http://www.igis.gov.au).

- organizarea de întâlniri periodice cu miniștrii responsabili și/sau directorii serviciilor;
- efectuarea inspecțiilor, atât regulate, cât și *ad hoc*, și vizitarea incintelor serviciilor de informații.

2.2.4 Puterea judecătorească

Dat fiind că serviciile de informații nu se situează deasupra legii, ele se află în jurisdicția instanțelor judecătorești. Deși rolul instanțelor judecătorești în raport cu munca de informații merită o atenție mai detaliată decât poate fi oferită aici, următoarele comentarii succinte pot fi utile.

Cu toate că puterea judecătorească are responsabilitatea de a susține statul de drept și de a asigura respectarea drepturilor omului, prin tradiție, judecătorii au încredințat executivului problemele de securitate națională din două motive. În primul rând, constituțiile și legislația care le reglementează plasează adesea problemele de securitate națională în competența exclusivă a executivului. În al doilea rând, mulți judecători consideră că instanțele judecătorești nu sunt incinte potrivite pentru dezvăluirea informațiilor confidențiale.[18] Chiar și așa, unele sisteme judiciare joacă un rol activ în supravegherea serviciilor de informații. În SUA, de pildă, extinderea drepturilor la un proces corect, de care beneficiază inculpații, a făcut ca judecătorii să examineze și mai detaliat conduita guvernului, iar Congresul a adoptat tot mai multe legi în domeniul intelligence, care au contribuit şi ele la o verificare sporită din partea judecătorilor.[19] În alte țări, în special acolo unde executivul s-a manifestat excesiv și autoritarist în numele securității naționale, judecătorii au devenit mai activi în susținerea drepturilor constituționale și a drepturilor omului.[20]

Supravegherea exercitată de puterea judecătorească asupra serviciilor de informații are patru forme principale, dintre care trei depășesc sfera supravegherii și intră în zona controlului. Mai întâi, legislația care le reglementează funcționarea impune serviciilor de informații care doresc să utilizeze măsuri speciale de investigare (cum ar fi interceptarea comunicărilor) să solicite o

---

18 Ian Leigh, „National courts and international intelligence cooperation” [„Instanțele judecătorești naționale și cooperarea internațională în domeniul intelligence”], în *International intelligence cooperation and accountability*, editori Hans Born, Ian Leigh și Aidan Wills (Londra: Routledge, 2011), p. 232.

19 Frederic Manget, „Another system of oversight: intelligence and the rise of judicial intervention” [„Un alt sistem de supraveghere: intelligence și intesificarea intervenției judiciare”], în *Strategic intelligence: A window into a secret world*, editori Loch Johnson și James Wirtz (Los Angeles: Roxbury, 2004), pp. 407–409.

20 Leigh, “National courts and international intelligence cooperation,” p. 232.

autorizație *ex ante* din partea judecătorului sau să se supună unei verificări judiciare *ex post*. Asemenea cerințe sunt importante fiindcă inițiază o verificare independentă privind legalitatea activităților intruzive ale serviciilor. În al doilea rând, judecătorii pot fi chemați să prezideze în procese penale care implică infracţiuni legate de munca de informaţii și să judece reclamații – constituționale, civile sau administrative – care implică probleme din domeniul intelligence. În al treilea rând, în unele state (în Franța, de exemplu), judecătorii de instrucție specializați în probleme de securitate pot efectua un control de supervizare asupra investigațiilor întreprinse de serviciile de informații. În al patrulea rând, ocazional, judecătorii pot deveni membri ai organismelor de supraveghere sau pot fi solicitați să prezideze comisii *ad hoc* de anchetă.

Primele trei roluri de mai sus pot fi calificate ca mijloace de control, deoarece dau judecătorilor puterea de a orienta activitățile serviciului de informații implicat. Cel de-al patrulea rol, prin comparație, este mai limitat, lipsindu-i, de obicei, puterea de a emite recomandări cu caracter de obligativitate.

2.2.5 Instituțiile de tip ombudsman

Forma cea mai frecventă de interacțiune între instituțiile de tip ombudsman și comunitatea de informații este gestionarea reclamațiilor împotriva serviciilor de informații, înaintate de orice persoană. În Olanda, de exemplu, oricine poate înainta ombudsmanului național o reclamație referitoare la „acțiuni sau pretinse acțiuni ale miniștrilor relevanţi, ale șefilor serviciilor (de informații), ale coordonatorului și persoanelor care lucrează pentru servicii și pentru coordonator.”[21] Inițial, reclamantul trebuie să informeze ministrul responsabil care cere apoi avizul Comisiei de Verificare a Serviciilor de Informații și de Securitate (CTIVD). Apoi, ombudsmanul național olandez investighează reclamația și remite „decizia sa în scris persoanei care a înaintat reclamația, menționând totodată argumentele care stau la baza ei în măsura în care securitatea sau alte interese vitale ale statului nu impun altceva.”[22]

Instituțiile de tip ombudsman tind să aibă atât avantajul independenței, cât și competențele legale necesare pentru a accede la informații relevante pentru investigațiile desfășurate. Din nefericire, există și tendința ca ele să dispună de un personal prea puțin numeros pentru a acoperi într-o manieră eficace zonele extinse de jurisdicție, ce înglobează frecvent nu doar comunitatea de

---

[21] Olanda, Legea din 7 februarie 2002, care prevede reguli referitoare la serviciile de informații și de securitate și modifică mai multe legi – *Intelligence and Security Services Act 2002* [*Lege privind serviciile de informații și de securitate – 2002*], Articolul 83, Paragraful 1, p. 31.

[22] Ibid., Articolul 84, Paragraful 1, p. 31.

informații, ci și forțele armate și, uneori, întreg guvernul. În consecință, instituțiile de tip ombudsman sunt afectate adesea de incapacitatea de a dedica suficiente resurse și expertiză pentru supravegherea serviciilor de informații.

2.2.6 Instituțiile supreme de audit

La fel ca și instituțiile de tip ombudsman, instituțiile supreme de audit (SAI) asigură verificarea externă independentă a conduitei serviciilor de informații. Concret, ele monitorizează aspectele financiare ale muncii de informaţii, stabilind dacă evidența documentelor în cadrul unui serviciu este corectă și exactă, dacă funcționarea controalelor interne e corespunzătoare și dacă cheltuielile efectuate de serviciu sunt conforme cu principalele reglementări în domeniu (a se vedea Wills – Instrumentul 8). În plus față de aceste responsabilități, instituțiile supreme de audit fac evaluări cost-eficiență, astfel încât legislatorii și membrii executivului să poată lua decizii în cunoștință de cauză privind modalitatea cea mai bună de structurare a bugetelor și priorităților serviciilor de informații.

2.2.7 Societatea civilă și mass-media

Deși se admite faptul că *societatea civilă* e un concept amorf, în general, ea este înțeleasă ca înglobând organizațiile autonome care se plasează în spațiul public între instituțiile statului și viața privată a indivizilor și comunităților. O astfel de definiție include, de exemplu, mediul academic, organizațiile neguvernamentale (ONG-urile), grupurile de interese și ordinele religioase. Un mare avantaj al organizațiilor din societatea civilă în efectuarea supravegherii serviciilor de informații este capacitatea lor de a analiza și critica fără restricții politicile guvernului.

La fel ca organizațiile societății civile, entitățile din mass-media utilizează expertiza independentă (adică neguvernamentală) pentru a oferi un feedback constant cu privire la acțiunile serviciilor de informații. Îndeosebi jurnaliștii de investigație au un rol esenţial în sesizarea conduitei incorecte, ilegale, ineficace și/sau ineficiente a serviciilor de informații. Odată sesizate, aceste cazuri de eșec sau acțiune reprobabilă devin adeseori obiectul unor anchete oficiale, conduse de comisiile parlamentare sau alte organisme independente de supraveghere, așa cum sunt organismele specializate de supraveghere, instituțiile de tip ombudsman sau instituțiile supreme de audit (SAI). În absența relatărilor făcute de mass-media, care atrag atenția asupra unor astfel de chestiuni, acestea ar putea să nu fie investigate niciodată.

Fie că sunt sesizări ale unor fapte reprobabile sau pur și simplu ştiri de presă despre politica executivului, relatările din mass-media tind totodată să plaseze pe agenda guvernului anumite probleme, făcând din ele subiecte de dezbatere publică. De pildă, seria de articole „Top Secret America" publicată de Washington Post, a dezvăluit expansiunea uimitoare a comunității de informații din SUA în deceniul care a urmat atacurilor din 11 septembrie 2001, dând naștere unei aprinse dezbateri publice despre raportul cost-eficiență al unei asemenea investiții.[23] Cu toate acestea, trebuie să se recunoască faptul că jurnalismul puternic politizat sau subiectiv poate prejudicia supravegherea serviciilor de informații.

2.3 CICLUL DE SUPRAVEGHERE A SERVICIILOR DE INFORMAȚII

Supravegherea se poate efectua în diferite momente. Se poate face la începutul unei operațiuni care a fost propusă, dar nu încă întreprinsă (supraveghere *ex ante*), se poate produce în timpul efectuării operațiunii (supraveghere pe parcurs), sau poate avea loc după terminarea acesteia (supraveghere *ex post*).

2.3.1 Supravegherea *ex ante*

Cele mai comune activități de supraveghere *ex ante* includ: crearea unui cadru legal cuprinzător pentru serviciile de informații și organismele care le supraveghează, stabilirea și aprobarea bugetelor serviciilor de informații și autorizarea operațiunilor de informații care depășesc un anumit prag de sensibilitate.

Pentru ca un cadru legal să fie eficace, el trebuie să stabilească cu claritate mandatul serviciului sau al organismului de supraveghere și competențele de care dispun aceste entități. Deși poate că nu este o supraveghere în sensul convențional, această activitate legislativă constituie un punct de plecare (și un element *sine qua non*) pentru orice sistem de supraveghere util. Fără mandate și competențe clar definite, serviciile de informații și organismele de supraveghere nu pot funcționa corect. (Crearea cadrului legal este abordată pe larg de Farson – Instrumentul 2).

Agențiile guvernamentale nu pot funcționa fără fonduri. Așa că parlamentul, care, într-o democrație, controlează utilizarea fondurilor publice, trebuie să adopte bugete anuale pentru toate agențiile guvernamentale, inclusiv pentru serviciile de informații. Bugetele propuse sunt, de regulă, prezentate comisiei parlamentare pertinente de către ministrul responsabil, care acționează în

[23] Dana Priest și William M. Arkin, „Top Secret America: A Washington Post Investigation" [„America strict secret: o investigație a cotidianului *The Washington Post*"], serie de patru articole în *The Washington Post*, iulie–decembrie 2010 (disponibil la http://projects.washingtonpost.com/top-secret-america).

consultare cu conducerea superioară a serviciilor, cu trezoreria și, în unele cazuri, cu instituția supremă de audit. (Procesul bugetar este discutat mai detaliat în Wills – Instrumentul 8.) Ulterior, membrii comisiei parlamentare fac o evaluare a bugetului propus din perspectiva politicii curente a executivului în domeniul intelligence. Deloc surprinzător, parlamentarii folosesc frecvent procesul bugetar ca pe o oportunitate de a critica politica executivului și prioritățile pe care acesta le-a stabilit pentru serviciile de informații.

Activitățile de intelligence care necesită o autorizare prealabilă implică de obicei utilizarea unor puteri speciale care încalcă drepturile individuale, ca, de exemplu, supravegherea electronică a comunicațiilor personale. Cel mai adesea, această formă de supraveghere *ex ante* este efectuată de un judecător, însă, în anumite situații, ea poate fi realizată de un organism de supraveghere care nu e judiciar sau este cvasi-judiciar, precum Comisia G10 din *Bundestag-ul* german (denumită astfel după Articolul 10 din legea fundamentală germană, care se referă la caracterul privat al poștei și telecomunicațiilor). (A se vedea Hutton – Instrumentul 5).

2.3.2 Supravegherea pe parcurs

Supravegherea pe parcurs poate include investigații, inspecții la fața locului, audieri periodice și raportarea regulată a activităților de către serviciile de informații și de înseși organismele de supraveghere. În plus, în unele state, judecătorii verifică periodic operațiunile în curs, de culegere a informațiilor, precum interceptarea convorbirilor telefonice, pentru a stabili dacă operațiunile în cauză se justifică în continuare.

În 2011, Comisia olandeză de Verificare a Serviciilor de Informații și de securitate (CTIVD) a raportat că activitățile ei de supraveghere pe parcurs au inclus verificări regulate ale operațiunilor de interceptare a convorbirilor telefonice, întreprinse de servicii, ale operațiunilor de control de securitate efectuate de servicii și ale prelucrării cererilor de acces la dosarele serviciilor. În plus, Comisia de Verificare a urmărit dacă serviciile și-au îndeplinit obligația legală de a notifica persoanele în cauză că au fost supuse utilizării unor măsuri speciale de investigare.[24] Un alt organism de supraveghere a serviciilor de informații cu un mandat specific de a efectua supraveghere pe parcurs este Comisia parlamentară norvegiană de supraveghere a serviciilor de informații (a se vedea Caseta 3).

[24] Olanda, Comisia de Verificare a Serviciilor de Informații și de Securitate (CTIVD), *Annual Report 2010–2011* [*Raport anual: 2010–2011*], pp. 8–9.

Caseta 3. Comisia parlamentară norvegiană de supraveghere a serviciilor de informații

Activitățile Comisiei parlamentare norvegiene de supraveghere a serviciilor de informații (Comisia EOS) sunt stipulate în „Legea privind monitorizarea serviciilor de informații, supraveghere și securitate” din 3 februarie 1995. Această lege stabilește rolul de „pură monitorizare” ce revine Comisiei EOS.[25] Potrivit legii, „Comisia nu poate să ordone organismelor monitorizate sau să fie consultată de acestea.”[26]

Secțiunea 3 a legii prevede că această Comisie EOS „va monitoriza cu regularitate practica serviciilor de informații, supraveghere și securitate în administrația publică și militară.” Secțiunea 4 permite comisiei, în îndeplinirea mandatului său, să intre în incinta acestor servicii, iar Secțiunea 5 dă comisiei permisiunea de a obliga martorii să compară în fața ei la audieri.

Mai mult, Secțiunea 8 obligă comisia să emită un raport neclasificat ca răspuns la orice reclamație pe care o primește și să înainteze rapoarte anuale Storting-ului (parlamentul norvegian), în care să-și prezinte activitatea. În plus, comisia poate elabora rapoarte periodice pe anumite subiecte dacă „se descoperă elemente care ar trebui aduse imediat la cunoștința Storting-ului.”[27] Această ultimă competență permite Comisiei EOS să efectueze o supraveghere serioasă pe parcurs a activităților desfășurate de serviciile norvegiene de informații.

2.3.3 Supravegherea *ex post*

Cele mai frecvente forme de supraveghere *ex post* sunt verificările tematice, verificările de caz, verificarea cheltuielilor (a se vedea Wills – Instrumentul 8) și verificările anuale. Totuși, în anumite situații, așa cum ar fi atunci când este sesizată o presupusă faptă reprobabilă, supravegherea *ex post* poate lua forma unei anchete *ad hoc*. Asemenea anchete sunt inițiate, în mod normal, pentru a cerceta și a face recomandări cu privire la anumite evenimente.

De exemplu, în 2004, guvernul canadian a lansat o anchetă specială privind rolul jucat de Poliția Regală Călare Canadiană (RCMP) în cazul Maher Arar, un cetățean canadian care, în urma extrădării sale de către SUA în Siria, a fost torturat (a se vedea Roach – Instrumentul 7). Ancheta a avut două aspecte: o verificare faptică și o verificare a politicilor RCMP. Scopul verificării faptice a fost de „a investiga și raporta cu privire la acțiunile oficialilor canadieni în legătură

[25] Norvegia, The Act relating to the Monitoring of Intelligence, Surveillance and Security Services, Act No. 7 of 3 February 1995 [Legea privind monitorizarea serviciilor de informații, supraveghere și securitate, Legea nr. 7 din 3 februarie 1995], Secțiunea 2.

[26] Ibid., Secțiunea 2.

[27] Ibid., Secțiunea 8, Paragraful 2.

cu ceea ce i s-a întâmplat lui Maher Arar."[28] Scopul verificării politicilor a fost de „a face recomandări pentru un mecanism independent și neutru de verificare a activităților RCMP legate de securitatea națională."[29] Structurarea investigațiilor *ex post* în această manieră, în două părți, este utilă deoarece stabilește adevărul despre ceea ce a fost deconspirat și, în același timp, oferă o oportunitate pentru formularea unor politici adecvate.

O altă zonă importantă a supravegherii *ex post* este gestionarea reclamațiilor (a se vedea Forcese – Instrumentul 9),[30] care se poate realiza în diverse formate instituționale. Deseori, reclamațiile sunt gestionate de puterea judecătorească, însă ele pot fi gestionate și pe cale nejudiciară, de entități precum instituțiile de tip ombudsman (de exemplu în Serbia), comisiile parlamentare (ca în Ungaria) sau organismele specializate de supraveghere (în Norvegia).

2.4 EVALUAREA SUPRAVEGHERII SERVICIILOR DE INFORMAȚII

Organismele de supraveghere a serviciilor de informații evaluează rezultatele serviciilor de informații, dar cine evaluează rezultatele sistemelor de supraveghere și cum se face această evaluare? Persoanele care supraveghează serviciile de informații și teoreticienii au început numai de curând să își pună astfel de întrebări, deoarece, printre alte motive, în multe state, sistemele de supraveghere a serviciilor de informații nu au fost înființate decât începând cu anii 1990.

Puține țări au apelat la evaluarea externă a sistemelor lor de supraveghere a serviciilor de informații. În Canada, o comisie specială a Camerei Comunelor a făcut acest lucru ca parte a unei evaluări după cinci ani a Legii privind Serviciul Canadian pentru Informații de Securitate,[31] în vreme ce în Olanda, la cererea CTIVD, un expert independent a efectuat o examinare similară a Legii privind

---

28 Comisia de anchetă privind acțiunile oficialilor canadieni în cazul Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* [*Un nou mecanism de verificare a activităților RCMP legate de securitatea națională*] (2006), p. 17.

29 Ibid., p. 17.

30 Deși reclamațiile se referă de regulă la evenimente care au fost deconspirate, trebuie precizat că, uneori, ele implică și operațiuni în curs sau care nu au trecut niciodată de faza de planificare.

31 Stuart Farson, „The Noble Lie Revisited:Parliament's Five-Year Review of the CSIS Act:Instrument of Change or Weak Link in the Chain of Accountability?" [„Nobila minciună reexaminată: verificarea de către parlament, după cinci ani, a Legii CSIS – un instrument al schimbării sau o verigă slabă în lanțul responsabilităților?"], în *Accountability for Criminal Justice: Selected Essays*, ed. Philip C. Stenning (Toronto: University of Toronto Press, 1995).

serviciile de informații și de securitate.[32] În plus, unele țări și-au evaluat sistemele de supraveghere ca parte a unor anchete parlamentare sau independente, referitoare la presupuse eșecuri sau acte reprobabile ale serviciilor de informații. Asemenea exemple includ Comisia 9/11 din SUA și ancheta cazului Arar în Canada.

Următoarele principii pot ghida cercetările viitoare asupra acestui important subiect, a cărui complexitate, în ansamblul său, depășește sfera lucrării de față:

- Legea de reglementare trebuie să prevadă verificări periodice ale sistemului de supraveghere a serviciilor de informații pentru a stabili dacă el servește în continuare scopului pentru care a fost creat.
- Aceste verificări periodice trebuie să vizeze întreg sistemul de supraveghere – inclusiv conducerea superioară a serviciilor de informații, executivul, parlamentul, puterea judecătorească, organismele independente de supraveghere, societatea civilă și mass-media.
- Asemenea verificări trebuie să stabilească dacă mandatele organismelor de supraveghere a serviciilor de informații, atunci când sunt evaluate în ansamblu, acoperă cele mai importante aspecte din activitatea serviciilor. Ele trebuie să determine, în special, dacă mandatele acoperă atât legalitatea, cât și eficacitatea conduitei serviciilor.
- Evaluarea organismelor specifice de supraveghere trebuie să se axeze pe capacitatea acestora de a trage la răspundere serviciile pe care le supraveghează. Cu alte cuvinte, competențele și resursele de care dispune un organism de supraveghere sunt suficiente pentru a-și executa mandatul? Mai precis, este acest organism îndeajuns de independent față de executiv și de serviciile de informații, poate accesa în suficientă măsură informațiile clasificate, are competențele necesare pentru investigare și dispune de un număr suficient de experți în stafful său ?

3. DE CE ESTE IMPORTANTĂ SUPRAVEGHEREA SERVICIILOR DE INFORMAȚII?

Cele trei rațiuni principale pentru care statele creează sisteme de supraveghere a serviciilor de informații sunt întărirea guvernanței democratice a serviciilor de informații (inclusiv a responsabilității lor în fața electoratului),

[32] Cyrille Fijnaut, *Het Toezicht op de Inlictingenen- en Veiligheidsdiensten: de noodzaak van krachtiger samenspel* [*Supravegherea serviciilor de securitate și de informații: necesitatea unei cooperări mai strânse*] (Haga, aprilie 2012) (în olandeză).

susținerea statului de drept și asigurarea eficacității și eficienței activității serviciilor.

3.1 GUVERNANȚA DEMOCRATICĂ ȘI RESPONSABILITATEA

Unul dintre principiile fundamentale ale guvernanței democratice este responsabilitatea instituțiilor de stat în fața electoratului. În plus, deoarece serviciile de informații folosesc fonduri publice, populația are dreptul să știe dacă aceste fonduri sunt utilizate în mod corect, legal, eficace și eficient.

Dată fiind natura confidențială a unei părți importante din activitatea de intelligence, serviciile de informații nu pot fi pe deplin transparente; așa încât, societatea trebuie să creeze un mecanism alternativ (altul decât examinarea publică) pentru a monitoriza, în numele electoratului, conduita acestor servicii. Cele mai frecvente mecanisme sunt comisiile parlamentare și organismele specializate de supraveghere, create de parlament în îndeplinirea obligației sale de a asigura existența unui sistem de pârghii și contraponderi pentru controlul tuturor agențiilor guvernamentale.

Un astfel de sistem trebuie să permită, în special, ca serviciile de informații să acționeze pentru apărarea securității naționale, și nu a securității guvernului în funcție. Într-adevăr, serviciile de informații nu trebuie să acționeze niciodată ca unelte ale unui partid politic, ci numai ca entități aflate în slujba populației.

Totodată, guvernanța democratică poate să întărească încrederea populației în munca serviciilor de informații dacă publicul larg știe că serviciile sunt supravegheate corespunzător de reprezentanții săi în parlament și de celelalte organisme de supraveghere.

3.2 APĂRAREA STATULUI DE DREPT

Serviciile de informații, ca orice altă agenție guvernamentală, sunt obligate să respecte și să apere statul de drept. Nici chiar existența unei amenințări la adresa securității naționale nu constituie un argument suficient pentru ca un serviciu de informații să încalce legea. Activitatea ilegală a unui serviciu de informații contravine statului de drept pe care serviciul are obligația de a-l proteja și, în plus, afectează reputația serviciului și pe cea a guvernului, în plan intern și internațional. Îndeosebi utilizarea puterilor speciale de către serviciile de informații trebuie monitorizată îndeaproape, datorită existenței unui potențial de încălcare a drepturilor omului.

În țările în care serviciile de informații au fost asociate în trecut cu abuzuri ținând de încălcarea legii și a drepturilor omului, este deosebit de importantă o supraveghere minuțioasă nu numai pentru a descuraja repetarea unor

greșeli, dar și pentru a genera încrederea și un sentiment de siguranță din partea populației față de servicii și guvern.

3.3 EFICACITATEA ȘI EFICIENȚA

Dat fiind că serviciile de informații joacă un rol vital în protejarea securității naționale și deoarece resursele lor sunt limitate, e important ca acele resurse să fie utilizate într-o manieră eficace și eficientă și nu risipite ori folosite inutil. Astfel încât, este necesar ca un sistem bine conceput de supraveghere să urmărească dacă serviciile de informații își folosesc într-adevăr resursele într-o manieră care asigură îndeplinirea priorităților ce le-au fost stabilite de guvern, obținând, în același timp, cea mai mare valoare în raport cu costurile suportate din banii contribuabililor.

De regulă, eficiența serviciilor este verificată atât de parlament, cu ocazia audierilor privind bugetul, cât și de instituția supremă de audit pe parcursul operațiunilor ei obișnuite de verificare a cheltuielilor. Natura secretă a activității de intelligence permite cu mai multă ușurință serviciilor de informații (în comparație cu alte agenții guvernamentale) să ascundă situațiile de fraudă și risipă; prin urmare, organismele de supraveghere trebuie să examineze cu deosebită atenție utilizarea fondurilor publice (a se vedea Wills – Instrumentul 8).

4. BUNE PRACTICI

Orice stat are nevoie să se asigure că serviciile sale de informații acționează în conformitate cu obligațiile lui legale internaționale, inclusiv cu cele cuprinse în *Carta Națiunilor Unite* și în *Convenția internațională cu privire la drepturile civile și politice*. În funcție de mandatul unui serviciu, pot fi, de asemenea, aplicabile acordurile internaționale referitoare la utilizarea puterilor polițienești. O cale pentru a respecta asemenea obligații este urmarea bunelor practici. În lucrarea de față, *bune practici* înseamnă prevederi legale naționale și internaționale, precum și structuri instituționale, proceduri și modele naționale care promovează o supraveghere eficace a serviciilor de informații.

Deoarece nu există un model de supraveghere a serviciilor de informații potrivit tuturor cazurilor, nu se poate emite pretenția că o anumită normă sau practică este indiscutabil cea mai bună. Mai degrabă, se poate spune că diverse modele și abordări, valabile în egală măsură, pot fi găsite în state din întreaga lume. Transferul bunelor practici de la un stat la altul poate fi dificil din cauza diferențelor în sistemele legale, politice și culturale; și chiar atunci când e posibil, procesul solicită, de obicei, adaptarea practicilor înainte de a putea fi aplicate de o manieră relevantă. Cu toate acestea, se pot identifica norme și

practici comune care contribuie la o supraveghere eficace a serviciilor de informații.

Caseta 4: Compilația Națiunilor Unite de bune practici în supravegherea serviciilor de informații

În 2010, pe baza cercetării întreprinse de DCAF, Raportorul special al Națiunilor Unite pentru promovarea și protejarea drepturilor omului și libertăților fundamentale în contextul combaterii terorismului a prezentat o compilație de bune practici privind serviciile de informații și supravegherea acestora.[33] În vreme ce compilația cuprinde 35 de bune practici privind baza legală, supravegherea și responsabilitatea, respectarea drepturilor omului și funcțiile serviciilor de informații, lista de mai jos se referă numai la bune practici în supravegherea acestor servicii.

PRACTICA 6. Serviciile de informații sunt supravegheate de un ansamblu de entități de supraveghere interne, guvernamentale, parlamentare, judiciare și specializate, ale căror mandate și competențe se bazează pe o legislație disponibilă public. Un sistem eficace de supraveghere a serviciilor de informații cuprinde cel puțin o instituție civilă care e independentă atât față de serviciile de informații, cât și față de executiv. Sfera combinată de competențe ale instituțiilor de supraveghere acoperă toate aspectele activității serviciilor de informații, inclusiv modul în care acestea respectă legea, eficacitatea și eficiența activităților lor, finanțele și practicile lor administrative.

PRACTICA 7. Instituțiile de supraveghere sunt abilitate și au resursele și expertiza necesare pentru a iniția și desfășura propriile lor investigații și dispun, totodată, de acces deplin și neîngrădit la informațiile, oficialii și facilitățile de care au nevoie pentru a-și îndeplini mandatele. Instituțiile de supraveghere se bucură de deplina cooperare a serviciilor de informații și a autorităților însărcinate cu aplicarea legii în procesul de audiere a martorilor și în obținerea documentelor și a altor probe.

PRACTICA 8. Instituțiile de supraveghere iau toate măsurile necesare pentru a proteja informațiile clasificate și datele personale la care au acces în decursul muncii lor. Sunt prevăzute penalități pentru încălcarea acestor cerințe de către membrii instituțiilor de supraveghere.

[33] Consiliul Națiunilor Unite pentru Drepturile Omului, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight* [*Raportul Raportorului Special pentru promovarea și protejarea drepturilor omului și libertăților fundamentale în contextul combaterii terorismului: Compilație de bune practici privind cadrul și măsurile legale și instituționale, care asigură respectarea drepturilor omului de către agențiile de informații în contextul combaterii terorismului, inclusiv supravegherea acestora*], United Nations Document A/HRC/14/46 (17 mai 2010).

În 2010, DCAF a pregătit pentru Raportorul special al Națiunilor Unite pentru promovarea și protejarea drepturilor omului și libertăților fundamentale în contextul combaterii terorismului un catalog de bune practici în supravegherea serviciilor de informații. Catalogul respectiv s-a bazat pe o analiză comparativă a constituțiilor, legilor, decretelor, rezoluțiilor parlamentare, anchetelor independente și deciziilor luate de instanțe judecătorești din mai mult de 50 de state (a se vedea Caseta 4).

5. RECOMANDĂRI

- Sistemele eficace de supraveghere utilizează atât organisme interne, cât și externe, inclusiv conducerea superioară a serviciilor, executivul, puterea judecătorească, comisiile parlamentare, organismele specializate, instituțiile de tip ombudsman, instituțiile supreme de audit, societatea civilă și mass-media.
- Luate împreună, mandatele organismelor care alcătuiesc sistemul de supraveghere a serviciilor de informații trebuie să se ocupe de corectitudinea, legalitatea, eficacitatea și eficiența întregii comunități de informații.
- Cel puțin un organism din sistemul de supraveghere a serviciilor de informații trebuie să fie civil, independent și să se situeze în afara acestor servicii și a executivului.
- Ce înseamnă exact un serviciu de informații trebuie definit într-o manieră funcțională. Și anume, orice organizație de stat ale cărei sarcini principale sunt culegerea, analizarea și diseminarea informațiilor privind securitatea națională este un serviciu de informații.
- Monitorizarea activității serviciilor trebuie să acopere întreg ciclul de supraveghere a activității de intelligence, care constă din supravegherea *ex ante*, pe parcurs și *ex post*.
- Eficacitatea unui sistem de supraveghere a serviciilor de informații trebuie evaluată regulat de organisme independente.
- Organismele de supraveghere a serviciilor de informații trebuie să comunice cu regularitate cu omologii lor din străinătate în scopul identificării și schimbului de bune practici.

INSTRUMENTUL 2

Înființarea unor sisteme eficace de supraveghere a serviciilor de informații

Stuart Farson



2

Înființarea unor sisteme eficace de supraveghere a serviciilor de informații

Stuart Farson

1. INTRODUCERE

Acest instrument examinează una din temele majore ale reformei sectorului de securitate: înființarea în statele aflate în tranziție a unor mecanisme eficace (în special mecanisme legislative) de supraveghere a serviciilor de informații și de stabilire a responsabilităților. O întrebare imediată ar fi următoarea: sunt oare mecanismele folosite de democrațiile consolidate modele adecvate pentru statele aflate încă în procesul de dezvoltare și extindere a formelor de guvernanță democratică? Răspunsul depinde de caracteristicile statului în tranziție ținând cont de considerente pertinente, care includ munca pe care serviciile de informații din statul respectiv au sarcina să o desfăşoare, sfera de cuprindere și dimensiunile activităților acestor servicii, precum și tabloul specific al ameninţărilor cu care se confruntă statul respectiv. În analizarea unor asemenea factori, trebuie să se țină totodată seama de aspecte de ordin mai general, îndeosebi de gradul în care acel stat a dezvoltat o cultură politică democratică și a încorporat practici democratice recunoscute.

Plasarea instituțiilor guvernamentale sub control democratic și tragerea lor la răspundere este una din cele mai importante sarcini ale democrației. Statele democratice diferă, totuși, în privința modului în care o aduc la îndeplinire. Unele se bazează pe parlamente pentru tragerea la răspundere a guvernului; altele au un sistem combinat, care înglobează o varietate de organisme specializate. Eficacitatea acestui proces, denumit de obicei supraveghere, depinde nu numai de puterea ce decurge din regulile legale și constituționale care determină ce anume poate fi examinat, unde, când și cât de des, dar și de măsura în care informațiile sunt puse la dispoziția organismelor de supraveghere. Fără capacitatea de a dobândi cunoștințe și de a păstra o memorie instituțională, niciun organism de supraveghere nu poate dezvolta expertiza

necesară pentru a ști unde să caute și ce întrebări să pună în scopul îndeplinirii obiectivelor sale.

Instituțiile independente, precum Centrul pentru Controlul Democratic al Forțelor Armate de la Geneva, au făcut mult în ultimii ani pentru dezvoltarea unor norme legale și bune practici în scopul reformării sectorului de securitate, în special în privința supravegherii serviciilor de informații.[1] În același timp, cercetătorii, pe lângă elaborarea unor studii despre anumite organisme de supraveghere, au încercat să analizeze funcțiile serviciilor de informații și ale activităţii de supraveghere a acestora dintr-o perspectivă comparată.[2] Totuși, sunt foarte puține studii care încearcă să discearnă eficacitatea în timp a modelelor de supraveghere.[3] În acest sens, au fost publicate numai studii ale unor exemple engleze și americane.[4]

---

[1] A se vedea, de exemplu, Hans Born (editor), *Parliamentary Oversight of the Security Sector: Principles, Mechanisms and Practices* [*Supravegherea parlamentară a sectorului securității: principii, mecanisme și practici*] (Geneva: DCAF, 2003); și Hans Born și Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* [*Responsabilizarea în domeniul intelligence: standarde legale și cele mai bune practici pentru supravegherea agențiilor de informații*] (Geneva: DCAF, Universitatea din Durham și Parlamentul Norvegiei, 2005).

[2] Pentru studii comparative, a se vedea Jean-Paul Brodeur, Peter Gill și Dennis Tollborg (editori), *Democracy, Law, and Security: Internal Security Services in Contemporary Europe* [*Democrație, lege și securitate: serviciile de securitate internă în Europa contemporană*] (Aldershot, UK: Ashgate, 2003); Thomas C. Bruneau și Steven C. Boraz (editori), *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness* [*Reforma în domeniul intelligence: obstacole în calea controlului democratic și a eficacității*] (Austin: University of Texas Press, 2007); Stuart Farson, Peter Gill, Mark Phythian, și Shlomo Shpiro (editori), *PSI Handbook of Global Security and Intelligence: National Approaches* [*Manualul Praeger Security International privind securitatea globală și intelligence: abordări naționale*] (Westport, CT: Praeger Security International, 2008); Greg Hannah, Kevin O'Brien, și Andrew Rathmell, *Intelligence and Security Legislation for Security Sector Reform*, Technical Report TR-288-SSDAT [*Legislația referitoare la intelligence și securitate pentru reforma sectorului de securitate*, Raport tehnic TR-288-SSDAT] (RAND Europe, 2005).

[3] Puține studii s-au ocupat de eficacitatea anumitor organisme de supraveghere pe parcursul unei perioade de timp. Acestea includ: Stuart Farson, „The Noble Lie Revisited: Parliament's Five-Year Review of the CSIS Act:Instrument of Change or Weak Link in the Chain of Accountability?" [„Nobila minciună reexaminată: verificarea de către parlament, după cinci ani, a Legii CSIS – un instrument al schimbării sau o verigă slabă în lanțul responsabilităților?"], în *Accountability for Criminal Justice: Selected Essays*, ed. Philip C. Stenning (Toronto: University of Toronto Press, 1995), pp. 185–212; Loch Johnson, *A Season of Inquiry: The Senate Intelligence Investiga-*

Numărul limitat de studii privind eficacitatea supravegherii constituie un factor restrictiv atunci când se pune problema de a recomanda o instituție de supraveghere în defavoarea alteia. Mai întâi, examinarea sistemelor de supraveghere care nu includ evaluări în timp are, prin comparație, o valoare limitată (valoarea pe care o oferă, în mod real, rezidă, probabil, în problemele pe care le descoperă prin studierea diferitelor abordări în materie de supraveghere). În al doilea rând, sistemele de supraveghere american și englez, care au fost studiate în timp, poate nu sunt cele mai bune modele pentru statele în tranziție. De exemplu, în cazul SUA, o examinare a sistemului de supraveghere a serviciilor de informații din această țară – date fiind sfera de acțiune și dimensiunile aparatului de intelligence, bugetele de mari dimensiuni și nivelul de implicare a sectorului privat –, are o valoare modestă pentru un stat în tranziție, unde condițiile sunt cu totul diferite.

Făcând distincție între diverse forme de guvernanță democratică, următoarea secțiune a acestui instrument analizează natura statelor în tranziție. Cea de-a treia secțiune aduce în discuție caracteristicile unei supravegheri eficace. Cea de-a patra secțiune identifică mai multe abordări instituționale ale supravegherii, care s-au dezvoltat în diverse state, atrăgând atenția asupra avantajelor și dezavantajelor lor. A cincea secțiune analizează obstacolele în calea unei supravegheri eficace, în vreme ce a șasea secțiune discută despre mandatele legale de care au nevoie organismele de supraveghere pentru a funcționa. Instrumentul se încheie cu mai multe recomandări de maximă importanţă.

2. STATELE ÎN TRANZIȚIE

Statele aflate în proces de dezvoltare a formelor democratice de guvernanță sunt frecvent numite state în tranziție. Ele împărtășesc experiența democratizării, însă, în rest, pot avea puține în comun, diferențiindu-se nu numai în

---

tion [*Un sezon de anchete: investigațiile Senatului în domeniul intelligence*] (Lexington: University Press of Kentucky, 1985); Kathryn S. Olmsted, *Challenging the Secret Government: The Post-Watergate Investigations of the CIA and FBI* [*Provocând guvernarea secretă: investigarea post-Watergate a CIA și FBI*] (Chapel Hill: University of North Carolina, 1996); și Kent Roach, „The Parliamentary Review of the Anti -Terrorism Act” [„Examinarea parlamentară a Legii împotriva terorismului”], în *Criminal Law Quarterly* 52 (mai 2007), pp. 281–4.

[4] Anthony Glees, Philip H.J. Davies, și John L. Morrison, *The Open Side of Secrecy: Britain's Intelligence and Security Commitee* [*Latura vizibilă a secretelor: Comisia britanică pentru informații și securitate*] (Londra: Social Affairs Unit, 2006); Frank J. Smist Jr., *Congress Oversees the United States Intelligence Community, 1947–1994,* [*Congresul supraveghează comunitatea de informații din Statele Unite, 1947-1994*], a II-a ediție (Knoxville: University of Tennessee Press, 1994).

privința punctului de la care au pornit, dar și în privința formei de democrație pe care au ales-o. Se poate ca unele să fi fost state democratice cândva, înainte de a trece printr-o perioadă totalitară; poate că unele sunt state nou înființate, create ca rezultat al dezintegrării unui stat mai mare; și poate că altele au trecut prin experiența unei dominări tribale, a unor divizări etnice profunde sau chiar printr-un război civil. Depinzând în parte de istoria lor diferită, direcțiile către care se vor îndrepta democrațiile acestor țări vor fi diferite. Unele vor crea un stat unitar; altele, un stat federal. Unele vor avea o președinție cu atribuții clare de control și verificări reciproce în raport cu puterea executivă; altele vor alege un sistem parlamentar care combină ramurile legislativă și executivă ale guvernării. Unele vor fi monarhii constituționale; altele – republici. Unele vor avea sisteme electorale majoritare cu vot uninominal; altele – o formă de reprezentare proporțională. Unele vor avea parlamente unicamerale; altele vor avea parlamente bicamerale. În plus, sistemele lor judiciare vor fi, adesea, diferite. Puse laolaltă, alegerile făcute de fiecare stat în tranziție vor avea un impact direct asupra tipului de cultură politică pe care îl dezvoltă.

Cultura politică a unui stat democratic, în special gradul în care idealurile democratice sunt acceptate de populație, determină căile prin care acele idealuri sunt puse în practică. De exemplu, membrii ramurii executive dintr-un stat pot fi mai dispuși să răspundă public pentru acțiunile lor decât membrii ramurii executive dintr-un alt stat. Astfel că și dezvoltarea responsabilității legislative va fi diferită de la un stat la altul. Progresul către o guvernanță democratică poate fi afectat în multe cazuri de o tendință spre de-democratizare [5] – alimentată de înclinația persistentă a celor aflați la putere de a folosi instrumentele statului pentru a-și menține puterea și, mai general, de corupție.

Chiar și terminologia referitoare la guvernanța democratică poate varia de la o țară la alta, îndeosebi atunci când e utilizată în contextul specific al supravegherii serviciilor de informații. De pildă, *responsabilitatea* este înțeleasă în general ca procesul prin care se dă socoteală; mai liber spus, ea implică transparență. Totuși, în statele Commonwealth-ului, care urmează modelul Westminster, *responsabilitatea* se referă și la o obligație constituțională, specifică miniștrilor responsabili din cabinet, de a prezenta în și pentru parlament rapoarte veridice privind acțiunile (sau lipsa de acțiune) a organizațiilor care sunt incluse în portofoliile lor ministeriale. Semnificații variabile au și alți termeni, precum *amenințări*, *riscuri*, *securitate națională*, *independență*, *discreție*, *competență*, *securitate*, *informații* și însăși *supravegherea*.

---

[5] A se vedea Charles Tilly, *Democracy* [*Democrația*] (Cambridge: Cambridge University Press, 2007).

3. O SUPRAVEGHERE EFICACE

Orice for legislativ, înainte de a înființa un sistem de supraveghere a serviciilor de informații, ar dori să estimeze dacă acel sistem are șansa de a fi eficace. Cu atât de multă literatură nouă referitoare la un asemenea subiect, s-ar putea crede că e o sarcină ușoară. Cu toate acestea, câteva comentarii care îndeamnă la prudență sunt binevenite. Deși unii cercetători au publicat recent studii documentare descriind funcțiile anumitor organisme de supraveghere, sunt puține studiile care analizează eficacitatea acestor organisme într-o manieră suficient de detaliată și de-a lungul unei perioade de timp îndeajuns de mari pentru a ajunge la concluzii semnificative. (Din păcate, studiile care au luat în considerare o perioadă mare de timp nu au reușit să formuleze criterii utile pentru aprecierea eficacității.)

Ceea ce tulbură și mai mult apele este tendința ramurilor executivă și legislativă ale guvernării de a urmări obiective diferite în supraveghere. Drept rezultat, multe țări democratice au dezvoltat un sistem combinat, în care mai multe organisme de supraveghere își propun să realizeze o varietate de obiective cărora le corespund diferite forme de verificare. Într-un asemenea sistem, comisiile legislative pot coexista cu organisme specializate de supraveghere, cu care uneori acționează coordonat, iar alteori, nu.

Oricare ar fi sistemul în vigoare, e important ca legislatorii să fie informați asupra activităților desfășurate de organismele de supraveghere, să primească informațiile la momentul oportun, iar rapoartele acestor organisme să fie accesibile imediat – ceea ce nu se întâmplă întotdeauna. Și, cel mai important, legislatorii trebuie să rămână în permanență conștienți de obiectivele ce trebuie îndeplinite prin supravegherea serviciilor de informații; altminteri, ei pot cădea în capcana unor abordări mai mult simbolice decât reale.[6] Scopul este, fără îndoială, unul simplu, același ca în cazul oricărei alte agenții guvernamentale. Nu e vorba de a controla munca serviciilor de informații,[7] ci de a le trage la răspundere în parlament, atât pe ele, cât și executivul, pentru acțiunile lor și pentru lipsa de acțiune, într-un mod pe care publicul să-l poată vedea și înțelege. Și totuși, acestea fiind spuse, elemente de control pot rezulta din cel

---

6 A se vedea Peter Gill, „Symbolic or Real? The Impact of the Canadian Security Intelligence Review Committee, 1984–88” [„Simbolic sau real? Impactul Comisiei de Verificare a Informațiilor de Securitate din Canada, 1984-88”], în *Intelligence and National Security* 4, Nr. 3 (1989) pp. 550–575.

7 În democrațiile parlamentare, controlul serviciilor de informații este în mod normal responsabilitatea executivului. Totuși, elemente de control parlamentar pot rezulta din competențele parlamentului de a aproba finanțarea serviciilor de informații și de a adopta legislația care reglementează funcţionarea serviciilor.

puțin două dintre responsabilitățile majore ale parlamentului – aceea de a examina și, ulterior, a aproba alocarea de fonduri publice pentru a acoperi costul activităților desfășurate de un serviciu de informații și aceea de a adopta sau amenda legislația care reglementează funcționarea serviciilor respective.

În îndeplinirea responsabilităților lor de supraveghere, legislatorii trebuie să-şi evalueze capacitățile, înclinațiile și limitele. Lipsa de timp, expertiza limitată și resursele insuficiente, toate afectează ceea ce se poate realmente obține. În consecință, legislatorii trebuie să se gândească serios la ceea ce doresc să obțină și cum se poate realiza acest lucru pe durata unui ciclu parlamentar de activitate. Poate că un organism specializat de supraveghere ar fi mai potrivit pentru anumite sarcini de supraveghere. Dacă răspunsul e afirmativ, care ar fi relația parlamentului cu acel organism?

În termeni foarte generali, parlamentele trebuie să fie implicate în supravegherea serviciilor de informaţii în două moduri distincte: primul se referă la conformare, celălalt, la eficacitate. Și anume, parlamentele trebuie să se asigure că serviciile de informații și contractorii acestora nu încalcă legea, regulamentele serviciilor sau politica guvernului. Ei trebuie să se asigure, totodată, că fondurile publice sunt folosite în mod adecvat și eficace.

Prea adesea, parlamentarii presupun că responsabilitatea lor primordială este să desfășoare o examinare *ex post facto* a activității serviciilor de informații – adică să o verifice după ce a fost efectuată. Ceea ce este numai parțial corect. Deși o verificare de substanţă poate și trebuie să aibă loc numai după efectuare, parlamentarii au totuși responsabilitatea de a face o anumită verificare şi înainte ca operațiunile în cauză să aibă loc, precum și pe parcursul desfăşurării lor. De exemplu, parlamentarii au responsabilitatea să se asigure că regulile și politicile guvernului, neapărat necesare, există înainte de desfășurarea operațiunilor. În mod asemănător, deși eficacitatea poate fi apreciată numai după efectuare, criteriile de capacitate și performanță trebuie să fie evaluate înainte și pe parcursul operațiunilor.

4. TIPURI DE ABORDARE A SUPRAVEGHERII

Această secțiune analizează trei tipuri de abordare a supravegherii folosite actualmente într-o serie de state democratice. Ele se referă la abordarea de către:

- comisiile legislative;
- inspectorii generali;
- organismele specializate de supraveghere.

Aici, termenul de *comisie legislativă* este utilizat generic pentru a include nu numai comisiile parlamentare, ci și comisiile unor foruri legislative care nu se referă la ele însele ca „parlamente.”

4.1 COMISIILE LEGISLATIVE

Comisiile legislative variază din punct de vedere al tipului şi competenţelor. În unele țări, cum sunt cele care urmează modelul Westminster, comisiile legislative pot reflecta un grad de combinare sau suprapunere între membrii aleși ai legislativului și cei care fac parte din structurile executive ale guvernării. În alte țări, nu există niciun fel de suprapunere.[8]

De la bun început, trebuie făcută o distincție netă între comisiile legislative din sistemele congresionale și cele din democrațiile parlamentare. Esențială e diferența în modul de abordare a responsabilității. În SUA, unde separarea puterilor încurajează fiecare ramură a guvernării să facă o verificare a celorlalte, Congresul este singurul care decide ce informații va primi și ce subiecte va examina în cadrul audierilor din comisiile sale. Puterile de a aloca fonduri publice și de a adopta legislația, acordate exclusiv Congresului, fac ca voinţa acestuia să fie, cu câteva excepții notabile, respectată. Astfel, comisiile din Congresul SUA audiază cu regularitate mărturiile tuturor categoriilor de oficiali de rang înalt din executiv, inclusiv pe cele ale şefilor administrativi ai serviciilor de informații, din partea cărora se așteaptă să dea toate răspunsurile la întrebări legate de politici şi administrare. (Membrii aleși din ramura executivă a SUA – anume președintele și vicepreședintele – nu depun mărturie în fața Congresului.)

Prin contrast, în majoritatea sistemelor parlamentare, ramura executivă are ultimul cuvânt în privința informațiilor clasificate care vor fi prezentate comisiilor legislative, pur și simplu pentru că partidul la putere, prin definiţie, controlează majoritatea din parlament. Există totodată o puternică diferență în aşteptările legate de cei care se vor prezenta în fața comisiilor și subiectele în privinţa cărora vor răspunde la întrebări. În unele jurisdicții parlamentare, membrii aleși ai ramurii executive se prezintă în fața comisiilor legislative pentru a răspunde la chestiuni privind politicile, în vreme ce alți oficiali din executiv se prezintă numai dacă doresc pentru a vorbi despre chestiuni administrative.

[8] În unele sisteme guvernamentale unde există separarea puterilor în stat, comisiile legislative nu pot chema să depună mărturie membrii aleși ai ramurii executive.

4.1.1 Abordările din Congres în SUA și Brazilia

În SUA, ca rezultat al investigațiilor Comisiilor Church şi Pike din anii 1970, Congresul a decis să înființeze comisii permanente pentru informații atât la Camera Reprezentanților, cât și la Senat. Aceste comisii au primit misiunea de a examina întreaga activitate a SUA din domeniul intelligence, analizând corectitudinea și eficacitatea acesteia. Întrunindu-se în locuri securizate și ajutate de un staff numeros, verificat din punct de vedere al securității, aceste comisii sunt împuternicite să-şi efectueze supravegherea înaintea, pe parcursul și după desfășurarea unei acţiuni. Responsabilitatea pentru examinarea activității interne în domeniul intelligence revine în prezent comisiilor din Congres, care supraveghează munca Departamentului de Justiție și a Departamentului pentru Securitate Internă. Stafful comisiilor, numit atât de partidul majoritar, cât şi de cel minoritar, oferă o serie de servicii membrilor din partidul care i-a numit. Acestea sunt completate cu serviciile unor importante agenții care acordă sprijin Congresului, cum sunt Serviciul de cercetare al Congresului și Oficiul Guvernamental de Conturi.

Brazilia oferă un alt exemplu de sistem congresional în contextul tranziţiei recente de la un regim militar la o democrație federală. Timp de cel puţin un deceniu după tranziţia din 1985, atenția noii ramuri executive din Brazilia a fost dominată de probleme presante, precum economia și nivelul ridicat al datoriei externe a țării. Aceste preocupări, împreună cu percepția larg răspândită că Brazilia nu avea dușmani străini, au făcut să nu pară urgentă reformarea sectorului de intelligence.[9] Totuși, de curând, Congresul brazilian nu numai că a restructurat sistemul, dar a înființat în Congres o serie de comisii care au rolul de a controla serviciile de informații. În 1999, el a creat ceea ce se numește acum Comisia mixtă pentru controlul activităților de intelligence (CCAI). De atunci, Congresul a mai creat patru comisii – inclusiv comisii de apărare atât la Camera Reprezentanților, cât și la Senat, Comisia pentru securitate publică împotriva crimei organizate, în Camera Reprezentanților, și Subcomisia permanentă pentru securitate publică, din cadrul Comisiei pentru constituție, justiție și cetățenie a Senatului. Toate au reușit să asigure o mai mare transparență – deși CCAI, în primii săi ani de existenţă, a avut de suferit ca urmare a lipsei de interes în rândul membrilor Congresului, a faptului că nu s-a reuşit agrearea

9 A se vedea Thomas C. Bruneau, „Intelligence Reforms in Brazil: Contemporary Challenges and the Legacy of the Past” [„Reformele din domeniul intelligence în Brazilia: Provocări contemporane și moștenirea trecutului”], în *Strategic Insights* VI, no. 3 (mai 2007) (disponibil la www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA485122).

regulamentului intern al comisiei, precum și din cauza insuficienţei resurselor tehnice şi a personalului de suport.[10]

4.1.2 Abordări parlamentare

Abordările parlamentare în supravegherea serviciilor de informaţii diferă nu numai faţă de abordările din Congrese, ci şi între ele.[11] Principalele diferențe se referă la accesul la informații clasificate, la stafful şi celelalte resurse pe care le au la dispoziţie, la mandatul comisiei și la modul în care sunt numiți membrii ei.

În practica actuală a parlamentelor, există nu mai puțin de cinci tipuri de abordare a supravegherii serviciilor de informaţii:

- comisii parlamentare în afara circuitului secretizat;
- comisii statutare de parlamentari;
- comisii parlamentare statutare permanente;
- comisii speciale statutare de verificare;
- comisii și sisteme combinate.

Comisii parlamentare în afara circuitului secretizat

În unele democrații parlamentare (precum Canada și Irlanda), ramura executivă nu stabilește nicio prevedere specială privind accesul comisiilor parlamentare la informaţii clasificate. Ca atare, orice persoană din cadrul circuitului secretizat – altfel spus, căreia i se permite să opereze cu informații clasificate – ar comite probabil o infracțiune dacă ar „face să se scurgă" o asemenea informație către un parlamentar. Drept rezultat, comisiile parlamentare din aceste democrații trebuie să lucreze fără o cunoaştere din interior a domeniului intelligence. Și totuși, ele nu sunt cu totul neputincioase. Deoarece dispun

[10] A se vedea Marco Cepik, „Structural Change and Democratic Control of Intelligence in Brazil" [„Modificări structurale și controlul democratic în domeniul intelligence în Brazilia"], în Thomas C. Bruneau și Steven C. Boraz (editori), *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness* (Austin: University of Texas Press, 2007) pp. 149–169.

[11] Pentru o analiză comparativă a sistemelor de supraveghere parlamentară din Uniunea Europeană, a se vedea Aidan Wills și Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* [*Supravegherea parlamentară a agențiilor de securitate și de informații în Uniunea Europeană*] (Bruxelles: Parlamentul European, 2011), în special, tabelele de la pp. 92–95.

de puteri depline de investigare și de resurse ale parlamentului, pot efectua verificări utile și pot aduce în atenţia guvernului probleme importante.[12]

Două avertismente suplimentare trebuie date în legătură cu această abordare. Mai întâi, există cu certitudine chestiuni care nu pot fi abordate în mod adecvat. De pildă, acolo unde organismele specializate de supraveghere semnalează anumite probleme îngrijorătoare, parlamentul nu poate fi ușor alertat în privința lor. În al doilea rând, fără un mandat precis, alegerea chestiunilor care vor face obiectul activității unei comisii va fi mai curând nesistematică. O dată cu schimbarea conducerii comisiei, se vor schimba și agenda acesteia și practicile și memoria instituțională.

Comisiile statutare de parlamentari

O a doua abordare, practicată în Marea Britanie, implică o comisie statutară de parlamentari.[13] Creată mai curând prin intermediul legislației decât ca prerogativă parlamentară, Comisia pentru informații și securitate (ISC) din Marea Britanie e alcătuită din parlamentari din Camera Comunelor și din Camera Lorzilor – selectaţi nu de partidele politice, ca în cazul comisiilor parlamentare, ci de primul ministru, căruia ISC îi raportează. Motivul este că ISC nu este, de fapt, o comisie parlamentară. Ea nu are, de exemplu, competențele de investigare ale unei comisii parlamentare și nu poate să se folosească de resursele și privilegiile obișnuite parlamentare. Este mai curând o comisie de parlamentari.

Avantajul ei principal rezidă în faptul că lucrează în interiorul circuitului secretizat, reunindu-se într-un mediu securizat și dispunând de un staff verificat din punct de vedere al securității. Alt avantaj îl reprezintă continuitatea. Membrii comisiei proveniți din Camera Lorzilor nu au nevoie, precum colegii lor din Camera Comunelor, să fie realeși; astfel, fac posibile o continuitate mai îndelungată și dezvoltarea unei memorii instituţionale.

Pe de altă parte, mandatul statutar al ISC e limitat, incluzând numai cheltuielile, administrarea și politicile principalelor servicii de informații. Tot limitate sunt și resursele ei de investigare. Deși au crescut de curând, ele continuă să lase de dorit. În consecință, abordarea din Marea Britanie tinde să descurajeze monitorizarea continuă a evenimentelor, care constituie, fără îndoială, un aspect important al supravegherii.

Eforturile de a aduce ISC sub control parlamentar au eșuat până acum, însă rolul partidelor politice a crescut. În prezent, ele influențează puternic selecția

[12] Comisia pentru securitate națională și apărare din Senatul canadian, atunci când era prezidată de Colin Kenny, s-a ocupat de o gamă largă de subiecte și a elaborat mai multe rapoarte importante, unele bazate pe activitatea desfăşurată *in camera.*

[13] Canada a analizat această abordare, dar nu a adoptat-o deocamdată.

membrilor comisiei și se alocă cu regularitate timpul necesar pentru dezbaterea versiunilor editate (publice) ale rapoartelor ISC.[14]

Comisiile parlamentare statutare permanente

Comisiile parlamentare statutare permanente pentru informații diferă de abordarea britanică prin aceea că ele sunt într-adevăr comisii parlamentare. Membrii lor sunt numiți de partidele politice și se pot folosi, în funcţie de nevoi, de resurse parlamentare.

Spre deosebire de ISC, al cărei staff o asistă după cum doreşte executivul, o comisie parlamentară permanentă poate să-și determine în mare măsură propria cale de acțiune nu numai în ceea ce privește stafful pe care îl angajează (cu condiția să fie verificat din punct de vedere al securității), dar și în privința locului de întrunire (atâta vreme cât e securizat).

Cerințele legate de componență variază de la o țară la alta. În Africa de Sud, de exemplu, regula o constituie reprezentarea proporțională și toate partidele politice importante trebuie să fie reprezentate în comisie. În Noua Zeelandă, atât primul ministru cât și liderul opoziției trebuie să fie membri ai acesteia. În Australia, comisia trebuie să aibă membri din ambele camere ale parlamentului federal.

Legislaţia care instituie asemenea comisii parlamentare permanente specifică, de regulă, care sunt organizaţiile pe care le pot verifica. Deși anumite activități sunt uneori excluse, domeniul lor de competenţă poate fi destul de larg. În Australia, de pildă, Comisia parlamentară mixtă pentru informații și securitate (PJCIS) are misiunea de a examina toate organizațiile importante de informații din țară, deși lista activităților pe care comisia nu le poate verifica este destul de lungă (a se vedea Caseta 1).

O diferență semnificativă între comisiile statutare de parlamentari și comisiile parlamentare statutare permanente rezidă în puterile și privilegiile lor. Cele din urmă pot acuza de sfidare părţile care nu respectă cerinţele comisiei, în special solicitările de prezentare a unor documente și înregistrări. În plus, legislația australiană prevede explicit că fiecare cameră a parlamentului poate trimite spre verificare către PJCIS „orice chestiune” care priveşte principalele servicii de informații.[15]

---

[14] Aceste rapoarte au fost pregătite iniţial la Secretariatul Cabinetului. Totuși, deoarece Secretariatul Cabinetului a fost perceput ca intrând într-un potențial conflict de interese, ele sunt pregătite în prezent într-un mediu securizat, considerat a fi mai independent.

[15] Ibid., Secțiunea 29(1)(b).

Caseta 1: Limitele mandatului Comisiei parlamentare mixte pentru informații și securitate din Australia

Funcțiile comisiei nu includ:

a. verificarea modului de culegere a informațiilor și de evaluare a priorităților de către Organizaţia Australiană pentru Informaţii de Securitate (ASIO), Serviciul Australian pentru Informaţii Secrete (ASIS), Organizația de Imagistică și Informații Geospațiale pentru Apărare (DIGO), Organizaţia de Informaţii pentru Apărare (DIO), Directoratul Semnale în domeniul Apărării (DSD) sau Oficiul de Evaluări Naționale (ONA); sau

b. verificarea surselor de informații, a altor forme de asistență operațională sau metode operaționale disponibile pentru ASIO, ASIS, DIGO, DIO, DSD ori ONA; sau

c. verificarea unor operațiuni specifice care au fost, sunt sau se propune a fi întreprinse de ASIO, ASIS, DIGO, DIO ori DSD; sau

d. verificarea informațiilor furnizate de un guvern străin ori de o agenție a unui guvern străin, acolo unde respectivul guvern nu consimte la dezvăluirea informațiilor; sau

e. verificarea unui aspect al activităților desfășurate de ASIO, ASIS, DIGO, DIO, DSD ori ONA, care nu afectează un cetăţean australian; sau

f. verificarea regulilor prevăzute în Secțiunea 15 a acestei Legi; sau

g. efectuarea unor anchete privind reclamații individuale împotriva activităților desfășurate de ASIO, ASIS, DIGO, DIO, DSD ori ONA; sau

h. verificarea conținutului sau a concluziilor evaluărilor şi rapoartelor elaborate de DIO sau ONA, sau verificarea surselor de informații pe care se bazează aceste evaluări sau rapoarte; sau

i. verificarea activităților de coordonare și evaluare asumate de ONA.[16]

Comisiile speciale statutare de verificare

În cel puțin o jurisdicție (Canada), viitoarele parlamente au fost obligate să înființeze comisii statutare de verificare, a căror misiune este examinarea legislaţiei din domeniul intelligence după un număr de ani de la intrarea ei în vigoare. Adoptarea în 1984 a „Legii privind Serviciul Canadian pentru Informații de Securitate” și a „Legii privind infracțiunile împotriva securității” a impus în mod special parlamentului să creeze o comisie pentru verificarea acestor legi, la cinci ani de la intrarea lor în vigoare.[17] În mod asemănător, „Legea împotriva

[16] Australia, *Intelligence Services Act 2001* [*Lege privind serviciile de informații* – 2001], Secțiunea 29(3).

[17] A se vedea Canada, Comisia specială pentru verificarea Legii CSIS și a Legii privind infracțiunile împotriva securității, în *Flux But Not In Crisis* (septembrie 1990).

terorismului" adoptată de Canada în 2001, a obligat parlamentul să înfiinţeze o comisie de verificare după o perioadă de trei ani.[18] În fiecare caz, mandatul comisiei era de a verifica prevederile şi modul în care funcţiona legea şi de a include în raportul său către parlament recomandări pentru orice modificări pe care le considera necesare.

Comisiile, care erau cu caracter *ad hoc*, au fixat un termen de un an pentru raport. Deoarece nu erau considerate a face parte din circuitul secretizat, au primit un sprijin redus din partea organismelor de supraveghere stabilite prin aceleaşi legi.[19]

Comisiile şi sistemele combinate

O serie de ţări au înfiinţat comisii combinate, ai căror membri includ atât parlamentari, cât şi persoane care nu fac parte nici din executiv, nici din legislativ.

Comisia pentru Protejarea Securităţii şi Integrităţii din Suedia

În Suedia, de exemplu, preşedintele şi vicepreşedintele Comisiei pentru Protejarea Securităţii şi Integrităţii (SAKINT) trebuie să fi ocupat funcţia de judecător sau să aibă o experienţă juridică echivalentă. Ceilalţi membri ai comisiei, în număr de până la 10, sunt numiţi dintre persoanele propuse de grupurile politice din parlamentul suedez (Riksdag) şi pot fi sau nu parlamentari.

SAKINT are două responsabilităţi principale: să supravegheze utilizarea de către agenţiile de combatere a criminalităţii a urmăririi secrete, a identităţilor false şi a tehnicilor speciale de investigare asociate; şi să supravegheze prelucrarea datelor cu caracter personal de către Serviciul de Securitate suedez. SAKINT îndeplineşte aceste responsabilităţi în primul rând prin inspecţii, al căror scop este să asigure respectarea legilor şi reglementărilor suedeze.

În desfăşurarea activităţilor sale, SAKINT e sprijinită de un staff condus de un director numit de guvern. Legea de înfiinţare a SAKINT a autorizat comisia să obţină informaţii şi asistenţă din partea organismelor administrative pe care le supraveghează. Comisia poate obţine informaţii şi de la organisme care nu

[18] A se vedea Kent Roach, „The Parliamentary Review of the Anti -Terrorism Act" [„Examinarea parlamentară a Legii împotriva terorismului"], în *Criminal Law Quarterly* 52 (mai 2007), pp. 281–4.

[19] A se vedea Stuart Farson, „The Noble Lie Revisited:Parliament's Five-Year Review of the CSIS Act:Instrument of Change or Weak Link in the Chain of Accountability?" [„Nobila minciună reexaminată: verificarea de către parlament, după cinci ani, a Legii CSIS – un instrument al schimbării sau o verigă slabă în lanţul responsabilităţilor?"], în *Accountability for Criminal Justice: Selected Essays*, ed. Philip C. Stenning (Toronto: University of Toronto Press, 1995), pp. 185–212.

sunt supuse supravegherii ei. SAKINT are sarcina de a prezenta anual un raport guvernului. În ceea ce privește Riksadg-ul, nu există o astfel de obligație.

Sistemul combinat din Germania

În Germania, sistemul de supraveghere a serviciilor de informații este combinat într-o manieră asemănătoare. Unii l-au numit „multilateral" deoarece cuprinde mai multe organisme care funcționează unul lângă altul.[20] Organismul principal este Comisia specială de control parlamentar (PKG), organul permanent de supraveghere a serviciilor de informații din camera inferioară a parlamentului german (Bundestag). Prin lege, PKG trebuie să se întrunească cel puțin o dată pe trimestru. Deși componența PKG reflectă configurația politică a Bundestag-ului, funcția de președinte revine anual, prin rotație, unui membru al majorității și unuia al opoziției. Membrii acestei structuri sunt asistați în munca lor de un secretariat format din șapte persoane. Ei își concentrează atenția asupra activităților celor trei servicii federale de informații și deliberează cu ușile închise. Comisia poate cita, pentru a depune mărturie, angajaţi din sectorul de intelligence, poate obține documente în funcție de necesități și poate intra oricând în incinta serviciilor. Ea trebuie să raporteze Bundestag-ului la mijlocul și la sfârșitul fiecărui mandat electoral.

Un al doilea organism este Comisia pentru chestiuni confidențiale, care răspunde de examinarea bugetelor serviciilor de informații (ale căror sume totale sunt comunicate Comisiei pentru buget a Bundestag-ului în vederea includerii lor în recomandările acesteia privind bugetul). Semnificativ este faptul că, uneori, PKG și Comisia pentru chestiuni confidențiale țin ședințe comune atunci când se discută chestiuni bugetare (a se vedea Wills – Instrumentul 8 pentru alte informații).

Componenta finală a sistemului combinat german este Comisia G10 – un organism independent, cvasi-judiciar, ale cărui decizii sunt obligatorii pentru serviciile de informații și guvern. Cei patru membri ai Comisiei G10, aleși de PKG, pot fi, dar nu neapărat, membri ai Bundestag-ului.

Comisia G10 a fost inițial creată pentru a autoriza și supraveghea interceptarea corespondenței și a telecomunicațiilor de către serviciile de informații. Totuși, atunci când, prin amendamentele la „Legea privind lupta împotriva terorismului", adoptată în 2007, s-au acordat noi competențe serviciilor de informații, s-a schimbat și rolul Comisiei G10. Acum, se cere serviciilor de informații

[20] A se vedea Shlomo Shpiro, „Parliamentary and Administrative Reforms in the Control of Intelligence Services in the European Union" [„Reforme parlamentare și administrative în controlul serviciilor de informații în Uniunea Europeană"], în *Columbia Journal of European Law* 4 (1998), pp. 545–578.

să obțină aprobarea prealabilă din partea Comisiei G10 înainte de a putea să solicite furnizorilor de servicii de telecomunicații date care ar dezvălui locul în care se află un telefon mobil activat, seriile sau codurile de card.

4.2 INSPECTORII GENERALI

Această secțiune examinează trei tipuri diferite de abordare în crearea prin lege a funcției de Inspector General (IG).[21] Cea dintâi, dezvoltată în SUA, a servit de atunci ca model pentru celelalte două. Totuși, acestea variază considerabil în privința entității care îl angajează pe Inspectorul General, a entității căreia îi raportează Inspectorul General și în privința subiectelor la care se referă respectivele rapoarte. Experiențele practice ale diferiților Inspectori Generali au fost și ele diferite, unii bucurându-se de un acces mai extins la personalul cheie și la informațiile necesare în comparație cu alții.

4.2.1 Inspectorul General al Agenției Centrale de Informații (CIA) din SUA

Cu toatecă „Legea privind Inspectorul General," din 1978, a cerut tuturor departamentelor majore din guvernul SUA să aibă inspectori generali, ea nu s-a aplicat Agenției Centrale de Informații, care avea deja propriul ei Inspector General. Înființat pentru întâia oară în 1952, Inspectorul General al CIA (IG-CIA) era, în 1978, încă numit de directorul agenției și, în opinia multora, insuficient de independent. Abia în 1989 au fost acordate, în sfârșit, IG-CIA o bază statutară și o mai mare independență. IG-CIA rămâne un angajat al CIA și continuă să raporteze directorului, dar poziția este ocupată în prezent de o persoană nominalizată de președinte, confirmată de Senat și care poate fi schimbată din funcție numai de către președinte.

Rolul IG-CIA este în principal acela de a promova economia, eficiența, eficacitatea și responsabilitatea în cadrul CIA. El sau ea își îndeplinește rolul prin realizarea de audituri, inspecții, investigații și verificări independente ale programelor și operațiunilor CIA. IG-CIA răspunde și pentru depistarea și prevenirea fraudelor, risipei, abuzului și administrării deficitare. Legat de raportare, IG-CIA i se cere să comunice cu promptitudine constatările și recomandările sale directorului agenției și comisiilor pentru informații din Congres. În cazul în care o

[21] A se vedea Geoffrey R. Weller, „Comparing Western Inspectors General of Intelligence and Security" [„Comparație între inspectorii generali pentru informații și securitate"], în *International Journal of Intelligence and CounterIntelligence* 9, no. 4 (1996), pp. 383–406.

constatare se referă la presupuse încălcări ale legii, IG-CIA trebuie să îl informeze și pe procurorul general.[22]

4.2.2 Inspectorul General al Serviciului Canadian pentru Informații de Securitate

Spre deosebire de IG-CIA, care e un angajat al agenției pe care o supraveghează, persoana care deține funcția de Inspector General în cadrul Oficiului Inspectorului General al Serviciului Canadian pentru Informații de Securitate (OIG-CSIS) nu este un angajat al serviciului, ci al Departamentului pentru Siguranța Publică, numit de cabinet și care raportează ministrului adjunct pentru siguranța publică. Mandatul OIG-CSIS, prevăzut prin „Legea privind Serviciul Canadian pentru Informații de Securitate" din 1984, este mult mai limitat decât cel al IG-CIA. El e în întregime axat pe respectarea legilor, regulamentelor și politicilor canadiene. O dată la 12 luni, OIG-CSIS trebuie să verifice raportul prezentat de directorul CSIS ministrului responsabil, referitor la activitățile operaționale ale serviciului. OIG-CSIS trebuie să certifice raportul, identificând orice activități neautorizate de legea CSIS sau care contravin dispozițiilor ministrului. În plus, OIG-CSIS trebuie să identifice orice activități care implică folosirea excesivă sau inutilă a puterilor CSIS.

Legea de reglementare conferă în mod expres OIG-CSIS dreptul de a primi de la directorul CSIS și de la alți angajați ai CSIS orice informații, rapoarte și explicații pe care le consideră necesare în vederea îndeplinirii îndatoririlor sale. Cu toate acestea, în practică, inspectorii generali au întâmpinat dificultăți în demersurile de a se întâlni cu directorii CSIS.

OIG-CSIS nu comunică direct cu parlamentul, nici chiar referitor la situații de nerespectare a prevederilor legale. În fapt, parlamentarii pot afla asemenea informații doar pe trei căi: dacă ministrul responsabil optează în mod voluntar să îi informeze; dacă obțin informațiile printr-o cerere în temeiul „Legii privind accesul la informații"; sau dacă informațiile sunt incluse într-unul din rapoartele anuale elaborate de Comisia de Verificare a Informațiilor de Securitate (SIRC), un organism specializat care funcționează totalmente separat de ramura executivă (a se vedea Secțiunea 4.3 de mai jos).[23]

---

[22] A se vedea Frederick M. Kaiser, „The watchers' watchdog: The CIA inspector general" [„Paznicul paznicilor: Inspectorul General al CIA"], în *International Journal of Intelligence and CounterIntelligence* 3, no. 1 (1989), pp. 55–75.

[23] Vreme de mai mulți ani, întârzierile în acordarea de către OIG-CSIS, a certificatelor de conformitate pentru SIRC au făcut ca raportul anual al comisiei să nu poată comenta aspectele referitoare la respectarea legii de către CSIS și, deci, să nu poată informa parlamentul în acest sens.

4.2.3 Inspectorul General australian pentru Informații și Securitate

Inspectorul General australian pentru Informații și Securitate (AIGIS) se aseamănă cu omologii săi din SUA și Canada prin faptul că are o bază statutară. Înființată în 1986 prin „Legea privind Inspectorul General pentru Informații și Securitate," funcția respectivă nu face parte din niciun departament ori agenție. Are statut independent și e inclusă în portofoliul propriu al primului ministru.

AIGIS, care e numit de guvernatorul general, are o sferă de acțiune mult mai largă decât inspectorii generali din SUA și Canada. În loc să examineze doar un serviciu, responsabilitatea sa se extinde asupra întregii comunități de informații din Australia. Deși acest inspector general îndeplinește, într-o anumită măsură, funcții diferite pentru servicii diferite, obligațiile sale principale sunt în număr de patru, și anume:

1. monitorizează respectarea legilor, dispozițiilor și liniilor directoare care guvernează activitățile diverselor servicii;
2. evaluează corectitudinea acestor activități;
3. evaluează eficacitatea acestor activități;
4. stabilește dacă vreuna din aceste activități nu e conformă cu un drept al omului sau contravine acestuia.

Poate că nu în mod surprinzător, AIGIS a dedicat prin tradiție majoritatea resurselor sale investigative activităţilor Organizaţiei Australiene pentru Informații de Securitate (ASIO), motivul fiind acela că jurisdicţia ASIO este, în principal, naţională și, astfel, există o mai mare probabilitate ca ASIO să încalce drepturile cetățenilor şi rezidenţilor australieni prin comparație cu serviciile australiene de informații externe și de apărare. (O estimare recentă sugerează că 60-70 % din resursele AIGIS sunt cheltuite pe programe proactive de inspecție).[24] În desfășurarea unei anchete complete, AIGIS poate să utilizeze și utilizează aceleași competențe de investigare prevăzute pentru comisiile regale de anchetă. Cu alte cuvinte, AIGIS poate obliga martorii să compară înaintea sa pentru a fi audiați și a depune mărturii veridice. Totodată, el/ea este împuternicit/ă să impună prezentarea obligatorie de documente, precum și să intre în incinta serviciilor respective. În același timp, siguranța menținerii sale

---

[24] A se vedea Ian Carnell și Neville Bryan, „Watching the watchers: How the Inspector-General of Intelligence and Security helps safeguard the rule of law" [„Păzindu-i pe paznici: cum contribuie Inspectorul General pentru Informații și Securitate la apărarea statului de drept"] (document prezentat la conferința *Safeguarding Australia 2005,* 12–14 iulie 2005) (disponibil la http://www.igis.gov.au/public_statments/conference_papers.cfm).

în această poziție e dată de faptul că poate fi înlăturată din funcție doar pentru un motiv întemeiat.

Legea de reglementare dispune ca AIGIS să prezinte un raport anual de activitate primului ministru, care trebuie să îl înainteze celor două camere ale parlamentului. Deși cei care au deținut anterior această funcție nu consideră că AIGIS este un organism de supraveghere capabil să provoace modificări,[25] recomandările pe care acesta/aceasta le face sunt, totuși, luate în serios de serviciile de informații și de miniștrii respectivi.[26]

În final, trebuie remarcat că, pe lângă verificările făcute de AIGIS și PJCIS (despre care s-a amintit mai sus), serviciile de informații din Australia sunt verificate și de Oficiul Național Australian de Audit.

4.3 ORGANISMELE SPECIALIZATE DE SUPRAVEGHERE

Organismele specializate de supraveghere sunt în mod normal înființate prin lege. Caracteristicile lor distinctive includ funcțiile pe care le îndeplinesc, gradul lor de independență față de executiv și parlament, entitatea căreia îi dau raportul, modul în care sunt selectați membrii lor și existența sau absența unor cerinţe privind calitatea de membru.

4.3.1 Comisia de Verificare a Informațiilor de Securitate și Oficiul Comisarului pentru Centrul de Securitate a Telecomunicaţiilor din Canada

Canada are două asemenea organisme specializate de supraveghere: SIRC și Oficiul Comisarului pentru Centrul de Securitate a Telecomunicaţiilor (OCSEC). SIRC, care funcționează în afara ramurilor executivă și legislativă ale guvernării, e format din maximum cinci membri care trebuie să fie, cu toții, membri ai Consiliului Privat și, deci, aflaţi sub un jurământ de păstrare a secretului. În plus, niciun membru al SIRC nu poate fi în acelaşi timp şi membru al parlamentului.[27] Inițial, s-a sperat că, în componența sa vor fi atrase persoane cu experiență în calitate de membri ai Consiliului Privat, care au ocupat funcţii de miniștri cu responsabilităţi în domeniu. Dar lucrurile nu s-au petrecut întot-

---

[25] În unele jurisdicții care urmează modelul Westminster, membrii executivului fac o distincție între examinare și supraveghere. Ei folosesc termenul de examinare pentru a desemna verificarea și termenul de *supraveghere* pentru a desemna o verificare însoțită de puterea de a efectua modificări. Astfel, în monitorizarea activităților din serviciile de informații, organismele de examinare pot doar să recomande modificări, în vreme ce organismele de supraveghere le pot impune ca obligatorii.

[26] A se vedea Ian Carnell și Neville Bryan, „Watching the watchers: How the Inspector-General of Intelligence and Security helps safeguard the rule of law."

[27] Inițial, s-a sperat că membrii SIRC vor fi foști miniștri cu responsabilități în domeniu, dar lucrurile nu s-au petrecut întotdeauna aşa.

deauna aşa. SIRC se întrunește într-un mediu securizat și dispune de un staff verificat din punct de vedere al securității. Pe lângă primirea certificatului de conformitate din partea Oficiului Inspectorului General-CSIS, SIRC are propriul său mandat de a asigura respectarea legii de către CSIS, inclusiv competența de investigare a reclamațiilor împotriva serviciului (a se vedea Caseta 2). În acest sens, SIRC poate trasa OIG-CSIS ori chiar serviciului sarcina de a efectua verificarea unor activități specifice.

Caseta 2: Mandatul Comisiei de Verificare a Informațiilor de Securitate din Canada

Funcțiile comisiei de verificare sunt următoarele:

a. verificarea, în general, a modului în care serviciul își îndeplinește obligațiile și funcțiile și, în legătură cu aceasta,
   i. verificarea rapoartelor directorului și a certificatelor Inspectorului General, transmise comisiei conform subsecțiunii 33(3);
   ii. verificarea dispozițiilor date de Ministru în temeiul subsecțiunii 6(2);
   iii. verificarea înțelegerilor făcute de serviciu conform subsecțiunilor 13(2) și (3) și 17(1) și monitorizarea furnizării de informații și produse de intelligence potrivit acelor înțelegeri;
   iv. verificarea oricărui raport sau comentariu care i-a fost prezentat conform subsecțiunii 20(4);
   v. monitorizarea oricărei cereri înaintate serviciului, conform paragrafului 16(3)(a);
   vi. verificarea reglementărilor; și
   vii. compilarea și analizarea statisticilor referitoare la activitățile operaționale ale serviciului;

b. stabilirea verificărilor de efectuat sau efectuarea verificărilor în conformitate cu secțiunea 40; și

c. efectuarea investigațiilor privind:
   i. reclamațiile făcute către comisie, în conformitate cu secţiunile 41 și 42;
   ii. rapoartele prezentate comisiei, potrivit secțiunii 19 din ”Legea cetăţeniei”; și
   iii. chestiunile repartizate comisiei conform secțiunii 45 din ”Legea drepturilor omului” din Canada.[28]

[28] Legea privind Serviciul Canadian pentru Informații de Securitate, R.S.C. 1985, Capitolul C-23, Secțiunea 38.

La efectuarea verificărilor, SIRC are drept de acces la orice informaţii gestionate de OIG-CSIS sau CSIS, pe care SIRC le consideră necesare pentru îndeplinirea obligațiilor şi funcțiilor sale – inclusiv rapoarte și explicații. SIRC poate prezenta rapoarte ministrului responsabil oricând doreşte; totuși, comisia trebuie să prezinte întotdeauna un raport anual pe care ministrul responsabil să-l poată înainta parlamentului. Deși SIRC poate să decidă conţinutul raportului anual, acesta nu trebuie să dezvăluie informații clasificate.

Inițial, s-a sperat că raportul anual al SIRC va oferi parlamentului informațiile de care avea nevoie pentru a efectua o supraveghere eficace în domeniul intelligence. În practică, totuși, SIRC nu a fost întotdeauna cooperantă.[29]

Atunci când Comisia specială a Camerei Comunelor pentru verificarea legii CSIS și a „Legii privind infracţiunile împotriva securității" (a se vedea Secțiunea 4.1.2 de mai sus) s-a întrunit pentru a analiza rolurile asumate de SIRC și, respectiv, de Oficiul Inspectorului General CSIS, membrii acesteia nu au reușit să înțeleagă de ce funcțiile OIG-CSIS nu puteau fi contopite cu cele ale SIRC. Ministrul responsabil de la vremea aceea s-a străduit mult să îi convingă pe membrii comisiei speciale de importanța Oficiului Inspectorului General CSIS și de necesitatea existenței celor două organisme. În consecință, comisia specială și-a schimbat orientarea și a renunțat să recomande desființarea Oficiului Inspectorului General CSIS. Totuși, câţiva ani mai târziu, un alt guvern a acceptat demisia celui care deținea postul – post pe care l-a lăsat ulterior vacant vreme de peste un an. De curând, guvernul și-a manifestat intenția de a contopi rolul OIG-CSIS cu cel al SIRC. Pretinzând că măsura preconizată urma să reducă cheltuielile administrative, el a argumentat totodată că activitatea de supraveghere va fi ameliorată.[30]

Până în 1996, când OCSEC a fost înființată prin decret, Centrul de Securitate a Telecomunicațiilor (CSE), serviciul canadian de culegere de informații prin interceptarea semnalelor, nu era supus niciunei supravegheri externe. Cinci ani mai târziu, parlamentul a adoptat „Legea împotriva terorismului," ca parte a

[29] A se vedea Stuart Farson, „The Noble Lie Revisited:Parliament's Five-Year Review of the CSIS Act:Instrument of Change or Weak Link in the Chain of Accountability?" [„Nobila minciună reexaminată: verificarea de către parlament, după cinci ani, a Legii CSIS – un instrument al schimbării sau o verigă slabă în lanțul responsabilităților?"], în *Accountability for Criminal Justice: Selected Essays*, ed. Philip C. Stenning (Toronto: University of Toronto Press, 1995), pp. 185–212.

[30] Bruce Cheadle, „Conservatives use budget bill to cut spy agency inspector general's office" [„Conservatorii folosesc proiectul legii bugetului pentru a reduce fondurile oficiului inspectorului general al agenției de spionaj"], în *Canadian Press*, 26 aprilie 2012.

unui proiect general de lege a Codului penal, care a oferit o bază statutară atât OCSEC, cât și CSE (care funcționase, ca şi CSEC, în temeiul unui decret). „Legea împotriva terorismului" a acordat OCSEC un mandat limitat, acela de a se asigura că CSE funcţionează în conformitate cu legislația canadiană. OCSEC e autorizat și să examineze reclamații împotriva agenției. Cerințele pentru ocuparea acestei funcţii includ experiența ca judecător la o instanţă superioară. Odată numit în funcţie, OCSEC poate fi demis numai dintr-un motiv întemeiat.

Similar cu OIG-CSIS și SIRC, OCSEC operează într-un mediu secretizat, într-o incintă securizată și cu un număr limitat de staff care a fost verificat din punct de vedere al securității. În plus, OCSEC se bucură de aceleași puteri de investigare acordate comisarilor în baza „Legii anchetelor." La fel ca SIRC, OCSEC trebuie să prezinte un raport anual pe care ministrul responsabil să-l poată înainta parlamentului.

Aceste două rapoarte anuale furnizează singurele informații pe care parlamentul canadian le primește direct de la OCSEC și SIRC. În nici unul din cazuri, guvernul nu este obligat să acționeze pe baza recomandărilor din rapoarte.

4.3.2 Comisia Permanentă pentru Verificarea Agențiilor de Informații din Belgia

Un organism specializat similar SIRC-ului efectuează supravegherea serviciilor de informaţii în Belgia. Cu toate astea, Comisia belgiană Permanentă pentru Verificarea Agențiilor de Informații (cunoscută sub denumirea de Comisia I) diferă de exemplul canadian în mai multe privințe care sunt importante. Mai întâi, mandatul său acoperă două servicii de informații (Securitatea de Stat, care e un serviciu civil, și Serviciul General pentru Informații și Securitate, omologul militar al Securității de Stat), precum și Unitatea de Coordonare pentru Evaluarea Amenințărilor.[31] În al doilea rând, mandatul Comisiei I nu se limitează la asigurarea conformității cu legile și reglementările, ci analizează și eficiența serviciilor, precum și coordonarea dintre ele. În al treilea rând, cei trei membri ai Comisiei I – care trebuie să fie verificați din punct de vedere al securității, să aibă o diplomă în drept și experiență profesională corespunzătoare – sunt numiți de Senatul belgian (și nu de Cabinet, ca în Canada). În fine, președintele comisiei trebuie să fie un magistrat.

Niciun membru al Comisiei I nu poate fi parlamentar, însă legea, în virtutea căreia funcţionează aceasta, stipulează obligația celor două camere ale parlamentului de a crea comisii permanente pentru monitorizarea activităţii Comi-

[31] Comisia I are și responsabilitatea de a se asigura că informațiile referitoare la terorism și extremism sunt transmise de Unitatea de Coordonare pentru Evaluarea Amenințărilor către autoritățile relevante politice, administrative și judiciare.

siei I și analizarea rapoartelor sale. Legea mai cere membrilor comisiilor parlamentare să ia măsuri de precauție adecvate legate de securitate și îi obligă să păstreze confidențialitatea informațiilor pe care le primesc chiar după ce nu mai deţin funcţia respectivă, atitudinea contrară fiind pedepsită prin lege.

5. OBSTACOLE ÎN CALEA UNEI SUPRAVEGHERI EFICACE

În statele aflate în tranziție, numeroşi factori pot constitui un impediment în stabilirea unor practici de supraveghere eficace a serviciilor de informaţii. Această secțiune se ocupă de cele mai frecvente obstacole.

5.1 RETICENȚA ÎN A TRAGE LA RĂSPUNDERE RAMURA EXECUTIVĂ

Cel mai important impediment pentru o supraveghere eficace este reținerea legislatorilor în a adopta şi aplica măsuri pentru tragerea la răspundere a ramurii executive. În statele în tranziție, unde, anterior, ramura executivă nu a fost trasă la răspundere, de regulă, legislatorii trebuie să experimenteze o diversitate de abordări înainte de a stabili care e metoda cea mai bună pentru ei. A se baza numai pe audierile din comisii pentru a asigura o supraveghere eficace se va dovedi, probabil, o metodă inadecvată. Experiența a arătat că sunt, de asemenea, necesare munca staffului, studiile de cercetare, vizitele pe teren și audierile *in camera*.

5.2 UN PROCES DIFICIL DE ÎNVĂŢARE

Activitățile din domeniile securității și intelligence diferă de majoritatea celorlalte funcții ale guvernului prin aceea că afectează și/sau implică aproape toate departamentele sau ministerele. Deoarece o supraveghere corespunzătoare necesită un grad ridicat de familiarizare cu funcțiile și practicile serviciilor de informații și cu modalitățile complexe în care ele interacționează cu alte agenții guvernamentale, procesul de învăţare este lent şi, deci, dificil pentru legislatori, care au de rezolvat multe alte solicitări, ce le ocupă timpul şi atenţia. Dezvoltarea expertizei necesare ia timp, în special dacă avem în vedere reticența generală a ofițerilor de informații în a-și împărtăși în detaliu cunoștințele.

5.3 LIPSA DE ÎNCREDERE

Dacă serviciile de informații și organismele de supraveghere a acestor servicii nu au încredere unele în altele, nu pot exista discuții sincere, schimburi semnificative de informații și nici o supraveghere eficace. Pentru construirea unor relații de încredere, organismele externe de supraveghere (în special comisiile legislative) trebuie să evite să se concentreze exclusiv pe respectarea legii. Limitarea în acest fel a supravegherii generează un mediu conflictual, pe princi-

piul „noi împotriva lor" și descurajează personalul din domeniul intelligence să vadă vreun beneficiu pe care i l-ar putea aduce procesul de supraveghere. Dimpotrivă, cel puțin în faza inițială, el percepe doar dificultăți considerabile.

Pentru ca o supraveghere să fie eficace, e necesar ca serviciile de informații să cunoască și beneficiile acesteia. De exemplu, un accent pe eficacitate poate aduce beneficii unui serviciu prin recomandări care încurajează executivul să-i pună la dispoziţie mai multe resurse. Serviciul poate, de asemenea, să vadă beneficiile supravegherii atunci când o comisie legislativă sau un organism specializat de supraveghere corectează o relatare de presă, care acuză în mod eronat membri ai serviciului de conduită incorectă sau pune sub semnul întrebării eficacitatea lor.

5.4 REFUZAREA ACCESULUI LA PERSOANE, LOCURI, DOCUMENTE ȘI ÎNREGISTRĂRI

Cel mai important obstacol în calea unei supravegheri eficace este refuzarea accesului la persoane, locuri, documente și înregistrări. Fără un asemenea acces, organismele de supraveghere nu pot funcționa în mod adecvat (a se vedea și Nathan – Instrumentul 3). Ele nu pot verifica dacă informațiile pe care le primesc din partea executivului sunt exacte și nici nu pot să dezvolte un plan corespunzător de investigare pe o anumită temă. Dimpotrivă, se pot baza numai pe ceea ce li se spune și pe ceea ce obțin din surse deschise.

5.5 PRESIUNEA TIMPULUI ȘI EFECTUL EI ASUPRA VERIFICĂRII

Presiunea timpului, resimțită de legislatori, poate avea un efect negativ asupra tipului de examinare pe care o întreprind. Studiile comisiilor de supraveghere din Congresul SUA au arătat că legislatorii, în loc să identifice ei înşişi problemele, sunt înclinați mai degrabă să preia probleme care au atras deja atenția opiniei publice[32] – și au motive întemeiate să procedeze astfel. Deoarece legislatorii sunt oameni ocupați, cu multe responsabilități (inclusiv propria lor realegere), ei au tendința să urmărească acele probleme care le oferă, cu cea mai mare probabilitate, un beneficiu politic personal. Verificarea serviciilor de informații, dat fiind că se desfășoară arareori în public, le oferă prea puţine oportunităţi de beneficii politice.

Capacitatea legislatorilor de a supraveghea serviciile de informații este obstrucționată și de însăși natura ramurii legislative. Timpul disponibil pentru

[32] A se vedea, de exemplu, Mathew D. McGubbins și Thomas Schwartz, „Congressional Oversight Overlooked: Police Patrols versus Fire Alarms" [„Supravegherea Congresului ignorată: patrule de poliție contra alarme de incendiu"], în *American Journal of Political Science* 28, no. 1 (februarie 1984), pp. 165–179.

supraveghere este limitat nu numai de munca pe care toți legislatorii trebuie să o desfășoare, ci și de ședințele forului legislativ. În cele mai multe jurisdicții, activitatea legislativă se oprește atunci când forul legislativ nu e în sesiune și în perioada alegerilor. O soluție parțială la această problemă este încredinţarea responsabilității de supraveghere unui organism specializat.

5.6 PARTIZANATUL

Procesul de supraveghere poate fi mult prea ușor obstrucționat de partizanat. De pildă, în SUA, când partizanatul devine excesiv, el poate zădărnici eforturile opoziției de a verifica un serviciu de informații prin amânarea sau controlarea activității comisiilor de supraveghere din Congres.[33] În mod asemănător, în cele mai multe sisteme parlamentare, partidul aflat la guvernare controlează agenda tuturor comisiilor legislative prin intermediul reprezentării majoritare. Pentru a contracara această dominaţie, ce reprezintă regula generală, unele sisteme solicită ca președintele comisiei pentru supravegherea informațiilor să fie un membru al unui partid de opoziție.

Alternarea președinției în acest mod și selectarea membrilor comisiei pe baza echilibrului corect între guvern și opoziție sunt modalități importante prin care partizanatul poate fi diminuat, iar cooperarea – promovată. În general, supravegherea funcţionează cel mai bine atunci când membrii comisiilor de supraveghere colaborează într-un efort colectiv de obţinere a unor rezultate ce slujesc interesului național.

5.7 RAPOARTE PREZENTATE CU ÎNTÂRZIERE DE ORGANISMELE SPECIALIZATE DE SUPRAVEGHERE

În situația în care sunt înfiinţate organisme specializate pentru a efectua diferite forme de verificare, proactive și de rutină, este foarte important ca rapoartele și analizele lor să fie puse la dispoziția legislatorilor la momentul oportun. Indiferent care sunt aspectele concrete din sfera intelligence pe care legislatorii le examinează ei înşişi, aceştia au totuşi nevoie să-și facă o imagine cât mai cuprinzătoare posibil pentru a duce la îndeplinire responsabilități extrem de importante, precum alocarea fondurilor publice şi examinarea legislaţiei în vigoare. Dacă legislatorii nu pot primi rapoarte la momentul oportun și nu-i pot chestiona pe membrii organismelor specializate cu privire la recomandările pe care le fac, capacitatea celor dintâi de a-și îndeplini responsabilităţile ce le revin va fi serios afectată.

---

[33] Marvin C. Ott, „Partisanship and the Decline of Intelligence Oversight" [„Partizanatul și declinul supravegherii serviciilor de informații"], în *International Journal of Intelligence and CounterIntelligence* 16, no. 1 (2003), pp. 69–94.

5.8 RESURSE NECORESPUNZĂTOARE

Capacitatea legislatorilor de a efectua o supraveghere eficace depinde în mare măsură de resursele care li se pun la dispoziţie. Cele mai importante resurse în acest sens sunt stafful și accesul. Așa cum s-a arătat mai înainte, legislatorii sunt oameni ocupați, cu o sferă largă de responsabilități. Fără ajutorul unui staff permanent, cu înaltă calificare și fără atitudini partizane, care să aibă cunoștințe vaste despre comunitatea de informații, legislatorii vor efectua, cel mai probabil, o supraveghere care, în cel mai bun caz, va fi limitată, axându-se mai curând pe audierile în comisie decât pe activitatea de investigare. Mai mult, pentru a efectua o supraveghere eficace, legislatorii au nevoie și de acces la o gamă extinsă de informații, inclusiv la servicii de cercetare și capacităţi de auditare.

Constituirea unui staff permanent de suport, fără atitudini partizane, poate contribui şi la dezvoltarea și păstrarea unei memorii instituționale. Dat fiind că expertiza în domeniul intelligence se obține în timp îndelungat, ritmul schimbării legislatorilor (care poate fi considerabil în unele sisteme) duce deseori la o pierdere de cunoştinţe şi experienţă. Din motive evidente, prezența unui staff permanent nepartizan diminuează acest obstacol în calea unei supravegheri eficace.

6. CONCEPEREA CADRULUI LEGAL ȘI INSTITUȚIONAL PENTRU UN SISTEM DE SUPRAVEGHERE

Mandatele de supraveghere trebuie să aibă cea mai amplă sferă posibil. Deși mandatul unui anumit organism de supraveghere ar trebui să depindă în mare măsură de locul pe care îl ocupă respectivul organism în ansamblul sistemului de supraveghere, luate împreună, aceste mandate trebuie să acopere o gamă largă de aspecte referitoare la serviciile de informații, de la administrare și operațiuni, la politici și mod de bugetare.

Pentru ca un sistem de supraveghere să fie eficace, el trebuie să se asigure că serviciile de informații pe care le monitorizează respectă legile, reglementările și politicile aplicabile și sunt eficace în îndeplinirea sarcinilor. Dacă monitorizarea conformității poate fi o misiune relativ simplă, evaluarea eficacității este mult mai complicată, fiindcă necesită o examinare cuprinzătoare a întregului sistem de intelligence şi securitate. În acest demers, nu e suficient să fie examinate pur și simplu agențiile care culeg informații. E necesar, de asemenea, să se verifice dacă liderii aleși: sunt angajați activ și constant în stabilirea strategiilor și responsabilităților pentru serviciile de informații; stabilesc cerinţe în materie de intelligence, care răspund ameninţărilor şi oportunităţilor curente;

stabilesc prioritățile ce trebuie urmărite; şi se asigură că diferitele componente ale sistemului de intelligence urmăresc aceste priorităţi.

Dacă se consideră sistemul de intelligence și securitate ca un întreg, este evident că, pentru a contribui la apărarea securității naționale, serviciile de informații trebuie să ofere guvernului, în orice moment, „cel mai bun adevăr” de care dispun. Totuși, munca de informații nu e o știință perfectă, iar „adevărul cel mai bun” poate avea uneori defecte serioase. Aceasta este natura muncii; dar chiar și așa, este esențial ca serviciile de informații „să-i spună puterii adevărul,” fără a ține seama de consecințele unui eșec. Pentru a promova și menține o astfel de atitudine în cadrul comunității de informații, serviciile au nevoie de sprijinul deplin al tuturor partidelor politice, chiar dacă ele fac obiectul unor critici obiective. Problema o constituie faptul că, în forul legislativ, alcătuit din partide politice, guvernele „în aşteptare” urmăresc, de regulă, să eclipseze partidul la putere, oferind puncte de vedere alternative. Așa că, tentația de a obţine un avantaj partizan învinge deseori dorința de cooperare. Din acest motiv, supravegherea serviciilor de informaţii are frecvent cea mai mare eficacitate atunci când este efectuată de organisme specializate de supraveghere care nu au o legătură directă cu executivul ori cu legislativul. O astfel de abordare oferă posibilitatea de a elimina politicul din munca de supraveghere a serviciilor de informaţii.

Cât despre respectarea legii de către serviciile de informații, organismele specializate de supraveghere ar trebui mandatate nu doar să verifice operaţiunile serviciului după ce acestea au avut loc, ci și să examineze în mod constant dacă legile, regulamentele și politicile aplicabile funcționează bine sau este necesar să fie revizuite. Totodată, aceste organisme ar trebui să fie obligate să investigheze reclamațiile împotriva serviciilor care au capacităţi de intruziune și coerciție sau să se asigure că reclamațiile sunt complet investigate de tribunalele competente (a se vedea Forcese – Instrumentul 9). Mai mult, ar trebui să li se ceară să prezinte regulat rapoarte tuturor autorităților competente, iar aceste rapoarte ar trebui să conțină, acolo unde este cazul, recomandări de remediere.

În ceea ce privește eficacitatea serviciilor de informații, organismele specializate de supraveghere trebuie să le evalueze atât capacităţile, cât și performanțele. Adeseori, evaluarea se face *post factum* (lecții de învățat), însă ea ar trebui să includă şi o componentă de parcurs, cu ajutorul căreia să se stabilească în ce măsură capacităţile de care dispune serviciul în prezent vor putea răspunde nevoilor preconizate de guvern pentru viitor. Instituțiile supreme de audit (SAI) dispun în mod obișnuit de capacităţile necesare pentru a concepe astfel de măsurători (a se vedea Wills – Instrumentul 8); însă, dată fi-

ind responsabilitatea lor curentă pentru întreaga gamă de operațiuni guvernamentale, e posibil să nu acorde în mod constant sectorului intelligence atenția cuvenită. În consecință, legislativul poate considera necesar să acorde SAI dispense speciale sau să înfiinţeze noi organisme de audit care să răspundă acestei cerințe.

La stabilirea mandatelor pentru organismele de supraveghere, legislatorii trebuie să se asigure că legislaţia de reglementare le permite acestora un acces suficient la toate componentele infrastructurii de securitate şi de intelligence. Procedând astfel, organismele de supraveghere vor putea face o evaluare a ansamblului capacităţilor de care dispune comunitatea de informații. Dacă nu au o sferă de acţiune atât de extinsă, executivul poate foarte uşor să paseze responsabilitățile și să evite o examinare atentă. O sferă extinsă de acţiune permite totodată celor care efectuează supravegherea să examineze relațiile structurale dintre organizațiile implicate şi modul în care relațiile respective funcţionează în practică și influențează costurile operațiunilor mixte.

În plus, legislaţia de reglementare ar trebui să garanteze membrilor organismelor în cauză o oarecare siguranță a funcţiei pentru a reduce potenţiala influenţare de către ramura executivă a procesului lor decizional. Altfel spus, ele pot ține din punct de vedere organizatoric de ramura executivă, însă nu ar trebui să facă parte efectiv din ea.

Astfel, se pune întrebarea: dacă legislativul înființează organisme specializate de supraveghere a serviciilor de informații, ce le mai rămâne legislatorilor de făcut în materie de supraveghere? Răspunsul are legătură cu trei responsabilități principale care revin forului legislativ în democrațiile parlamentare, și anume:

- dezbaterea și adoptarea legislației;
- aprobarea cheltuirii de fonduri publice de către departamentele și agențiile guvernamentale;
- tragerea la răspundere a guvernului pentru acțiunile sale sau pentru lipsa acestora.

Toate aceste responsabilități impun ca legislatorii să fie implicați activ în activitatea de supraveghere a serviciilor de informaţii. Pentru a-şi putea îndeplini obligațiile privind adoptarea legislației, aprobarea bugetului și stabilirea responsabilităţilor, membrii comisiilor legislative vor avea nevoie nu numai de acces, la momentul oportun, la rapoartele organismelor specializate de supraveghere, dar și de competenţa de a pune întrebări membrilor acestora pe baza rapoartelor pe care le prezintă. În plus, legislatorii vor avea uneori nevoie să desfășoare propriile lor investigații, atunci când au apărut probleme ce afec-

tează încrederea populației în serviciile de informații. Totodată, e necesar ca legislatorii să efectueze verificări de rutină ale activităților desfășurate de organismele specializate de supraveghere pentru a se asigura că acestea funcționează în mod eficace și dispun de resurse adecvate.

În fine, după cum s-a menționat în secțiunea 5.4, fără acces la persoane, locuri, documente și înregistrări, nu poate exista o supraveghere eficace. Prin urmare, cea mai importantă competență a unui organism de supraveghere este dreptul de acces, acordat în mod obligatoriu. Deși legislativul poate avea drept de acces, în general, comisiile legislative pot fi împiedicate să acceseze informaţii, personal şi medii de lucru cu caracter secret, deoarece condițiile necesare pentru un astfel de acces nu au fost prevăzute ferm în legea statutară.

7. RECOMANDĂRI

Orice legislaţie prin care se instituie un sistem de supraveghere a serviciilor de informaţii trebuie să includă în special următoarele aspecte:

Înființarea unei comisii legislative căreia să i se garanteze accesul la persoane, locuri, documente și înregistrări.

Legea de înfiinţare a acestei comisii trebuie să specifice puterile ei în privința accesului – așa cum sunt puterea de a trimite citații, puterea de a obliga la depunerea unei mărturii sub jurământ sau declaraţie solemnă, puterea de a intra în, şi de a cerceta incinta serviciilor de informații. Ea trebuie să specifice totodată cine poate deveni membru al comisiei și care sunt resursele de care va dispune comisia. Aceste două obiective ale ei, definite prin lege, ar trebui să prevină abuzurile din partea serviciilor de informații și de securitate și să amelioreze eficacitatea, eficiența şi economicitatea operațiunilor lor. În plus, comisia ar trebui să poată trasa oricărui organism de suport sarcina de a-și asuma proiecte de supraveghere, pe care ea nu are nici competența, nici răgazul de a le urmări; astfel de proiecte vor trebui finalizate și raportate într-o perioadă rezonabilă de timp.

Obligațiile ce-i revin comisiei trebuie să includă cerinţa ca supravegherea să se desfăşoare într-un mediu securizat. Membrii și stafful ei trebuie să fie verificați din punct de vedere al securității și să declare sub jurământ că nu vor divulga informații clasificate.[34] În plus, deși are permisiunea să prezinte rapoarte pu-

[34] Verificarea de către serviciile de securitate a legislatorilor și a altor persoane care dețin funcții importante (precum judecătorii) poate pune probleme constituționale din punctul de vedere al separaţiei puterilor. Și anume, este în general nepotrivit ca un membru al executivului să decidă dacă un membru al legislativului sau al ramurii judiciare corespunde poziției ocupate. Din motive evidente, o formă de verificare

blice oricând dorește, comisia ar trebui să fie obligată să elaboreze cel puțin o dată pe an un raport care va fi înaintat forului legislativ și pus la dispoziția opiniei publice. Toate rapoartele de acest fel trebuie să fie verificate de servicii pentru cazul în care ar conține materiale clasificate, însă decizia finală în privința subiectelor care vor fi incluse ar trebui să revină comisiei.

Legea ar trebui să stipuleze și efectuarea de către comisie a unor examinări periodice ale legilor referitoare la securitatea națională pentru a stabili dacă ele funcționează așa cum s-a dorit și continuă să reflecte amenințările și tehnologiile curente. Ea ar trebui să includă pedepse specifice pentru membrii comisiei și stafful care divulgă informații. În fine, ar trebui să-i autorizeze pe membrii comisiei să creeze comisii *ad hoc* de anchetă atunci când se impune expertiză din exterior sau când există probabilitatea ca o problemă să aibă un puternic caracter partizan.

Înființarea unui organism independent pentru examinarea reclamațiilor împotriva unui serviciu de informații.

Un astfel de organism trebuie să fie primul punct de contact pentru oricine ar face o reclamație împotriva unui serviciu de informații. Legea de reglementare ar trebui să prevadă măsuri specifice de protecție pentru informatorii interni. Aceștia trebuie protejați, cu condiția să nu fi dezvăluit informații clasificate ce nu au devenit în prealabil publice și să fi făcut dezvăluirile respective cu bună credință. Măsurile de protecție trebuie să se aplice, de asemenea, dacă dezvăluirile au fost considerate a fi de interes public. Mai mult, organismul trebuie să aibă și puterea de a examina cazuri individuale după ce au fost soluţionate, pentru a se asigura că informatorii interni nu au suferit repercusiuni care le-au afectat slujba.

---

este necesară pentru oricine va lucra de regulă cu informații clasificate. Din fericire, există mai multe căi pentru a ocoli problema constituțională. Puterea legislativă și cea judecătorească pot efectua propriile lor verificări informale, de genul celor care au loc atunci când o persoană e numită în funcţia de ministru; alternativ, ele pot folosi firme de securitate din afara sistemului pentru verificări mai formale. O asemenea verificare are trei beneficii importante: Întâi, serviciile de informații vor avea mai multă încredere și vor fi mai cooperante cu organismele de supraveghere ai căror membri au fost verificați. În al doilea rând, partenerii străini sunt mai dispuși să facă schimb de informații dacă sunt siguri că informațiile pe care le furnizează nu vor fi dezvăluite de organisme de supraveghere care nu au fost verificate. În al treilea rând, studiile privind devianța elitelor arată că „există mere stricate în toate butoaiele.” Judecătorii au fost corupți, membrii organismelor de supraveghere au fost siliți să demisioneze în urma unor conflicte de interese, iar legislatorii au fost găsiți vinovați de trădare. Verificarea poate îndepărta aceste „mere stricate” înainte ca ele să provoace vreun rău.

Crearea unuia sau mai multor organisme de supraveghere pentru a efectua o supraveghere, în principal, dar nu exclusiv, proactivă.

Aceste organisme trebuie să se poată întâlni și discuta liber între ele și cu comisiile legislative, cu condiția ca asemenea întâlniri să aibă loc în medii securizate. Ele pot răspunde și necesităților executivului, însă scopul lor primordial trebuie să fie asistența acordată comisiilor legislative în prevenirea abuzurilor de putere și stimularea unei mai mari eficacități. Cu toate că aceste organisme de supraveghere trebuie să fie capabile să-și dezvolte propriile lor planuri și grafice de activitate, ele trebuie să se orienteze și în funcție de dispozițiile primite din partea comisiilor legislative și a ramurii executive. Examinarea pe care o efectuează poate avea loc înainte de evenimentele pe care au decis să le verifice, pe parcursul sau după încheierea lor.

INSTRUMENTUL 3

Transparența, secretizarea și supravegherea în domeniul intelligence într-o democrație

Laurie Nathan



3

Transparența, secretizarea și supravegherea în domeniul intelligence într-o democrație

Laurie Nathan [1]

1. INTRODUCERE

Existența serviciilor de informații în țările democratice dă naștere unui paradox politic. Pe de o parte, serviciile sunt înființate pentru a proteja statul, cetățenii și alte persoane aflate în jurisdicția acestuia, precum și ordinea democratică; şi în acest scop li se acordă puteri și competenţe speciale. De obicei, în temeiul legislației, serviciile sunt autorizate să obțină informații confidențiale prin intermediul urmăririi, interceptării comunicațiilor și al altor metode care încalcă dreptul la viață privată, să întreprindă operațiuni sub acoperire pentru contracararea ameninţărilor la adresa securității naționale și să desfăşoare operaţiuni cu un nivel înalt de secretizare.

Pe de altă parte, serviciile de informații și membri ai executivului pot abuza de aceste puteri și competenţe pentru a submina siguranţa unor persoane şi pentru a compromite procesul democratic. Contravenind legii, pot încălca drepturile omului, pot interveni în activități politice legale și pot favoriza sau prejudicia un partid ori un lider politic. Îi pot intimida pe oponenții guvernului, pot crea un climat de frică și pot fabrica sau manipula informații pentru a influența deciziile guvernului și opinia publică. Totodată, pot abuza în folos personal de fondurile și metodele din domeniul intelligence.

---

[1] Acest instrument se bazează pe experiența și cercetările mele în calitate de membru al Comisiei ministeriale de verificare a serviciilor de informații, înfiinţată de ministrul pentru informații din Africa de Sud în 2006. Instrumentul se bazează și pe lucrarea lui L. Nathan *Lighting up the Intelligence Community: A Democratic Approach to Intelligence Secrecy and Openness* [*Comunitatea de informații adusă la lumină: o abordare democratică a caracterului secret și deschis al informaţiilor*], document orientativ (Birmingham, UK: Global Facilitation Network for Security Sector Reform, 2009).

Date fiind pericolele menționate, țările democratice se confruntă cu provocarea de a crea reguli, sisteme de control şi mecanisme de supraveghere pentru a diminua potențialul de conduită ilegală și abuz de putere și pentru a se asigura că serviciile de informații își îndeplinesc responsabilitățile în conformitate cu constituția și legislația.

Aceste obiective, valabile şi pentru organismele care controlează și supraveghează alte organizații de stat, sunt foarte dificil de realizat în sfera intelligence din cauza înaltului nivel de secretizare care înconjoară serviciile de informații și operațiunile lor. Secretizarea inhibă monitorizarea și verificarea efectuate de organismele de supraveghere, sufocă examinarea publică și facilitează ascunderea de către ofițerii de informații a greșelilor de conduită.

Instrumentul de față prezintă aspecte referitoare la caracterul secret și caracterul deschis al informațiilor și la furnizarea de informații, raportate la organismele de supraveghere a serviciilor de informații. Aceste organisme includ parlamentul, o comisie parlamentară de supraveghere a serviciilor de informații, puterea judecătorească, o instituție supremă de audit (SAI), un inspector general independent pentru informații (ca în Australia, Noua Zeelandă și Africa de Sud) și un organism specializat de supraveghere a serviciilor de informații (precum Comisia de Verificare a Serviciilor de Informații și de Securitate din Olanda). Instrumentul aduce în atenţie dezbaterea politică și conceptuală referitoare la secretizarea și transparența informațiilor, prezintă bune practici privind legislația ce reglementează protejarea informațiilor, precum și accesul la ele și discută despre informațiile pe care au nevoie să le cunoască parlamentul și celelalte organisme de supraveghere. Capitolul se încheie cu un set de recomandări.

Deşi discuțiile asupra caracterului secret al informațiilor se axează, în general, pe ceea ce nu trebuie dezvăluit, acest instrument explorează, într-o manieră mai pozitivă, zonele din domeniul intelligence, care ar trebui dezvăluite în interesul unei supravegheri eficace și al guvernanței democratice.

De asemenea, trebuie subliniat de la început că o secretizare excesivă dă naștere suspiciunilor și temerilor față de organizațiile de informații, reducând sprijinul public în favoarea lor. Într-o democrație, spre deosebire de un stat polițienesc, agențiile de informații, pentru a avea succes, trebuie să se bazeze pe cooperarea populaţiei, şi nu pe coerciție și teroare. Oferirea unor informaţii mai ample despre servicii este de natură să le aducă în atenţie de o manieră pozitivă, să diminueze îndoiala şi temerile induse de caracterul secret, să amelioreze cooperarea cu serviciile și, prin urmare, să le sporească eficacitatea.

2. PROBLEMA TRANSPARENŢEI ŞI SECRETIZĂRII ÎN SUPRAVEGHEREA SERVICIILOR DE INFORMAŢII

Cea mai importantă și controversată chestiune legată de guvernanța democratică a serviciilor de informații este cea a caracterului secret. Și asta, deoarece cu cât este mai mare nivelul de secretizare, cu atât este mai dificil să se stabilească și să se evalueze caracteristicile și performanțele serviciilor. În absența unor informații adecvate, organismelor de supraveghere le este imposibil să determine și să dezbată în mod real rolul și orientarea serviciilor, necesitatea unor reforme în domeniul intelligence, precum și întrebarea-cheie dacă serviciile apără ori subminează siguranța și libertatea cetățenilor și ale altor persoane aflate sub jurisdicția unui stat.

Subiectul este disputat pentru că i se asociază puternice presiuni care intră în competiție. Pe de o parte, anumite aspecte din comunitatea de informații și activitățile ei trebuie să rămână secrete, pentru a evita compromiterea operațiunilor și a vieții ofițerilor de informații, precum și a surselor lor. Pe de altă parte, secretizarea se află în antiteză cu guvernanța democratică, împiedicând responsabilizarea deplină și oferind un teren fertil pentru abuz de putere, ilegalităţi și o cultură a impunității.

Secțiunea aceasta studiază dezbaterea referitoare la transparenţă şi secretizare și prezintă o abordare democratică. Astfel de chestiuni sunt de o mare însemnătate pentru parlament. Dată fiind implicarea sa în elaborarea şi aprobarea legilor și politicilor care reglementează caracterul secret și accesul la informații, parlamentul joacă un rol major în stabilirea măsurii în care domeniul intelligence este supus sau nu examinării publice. Mai mult, nu numai că parlamentul are sarcina de a trage la răspundere executivul și organele statului, dar este el însuși răspunzător față de populație și are obligația de a-i informa pe cetățeni despre comunitatea de informații. În consecință, dezbaterile parlamentare privind legile, politicile şi bugetele serviciilor de informații trebuie să se desfășoare cu ușile deschise.

2.1 MOTIVAȚII PENTRU SECRETIZAREA INFORMAȚIILOR

Caracterul secret este o trăsătură intrinsecă și necesară a serviciilor de informații, datorită naturii mandatului și funcțiilor lor. Serviciile se ocupă de amenințările convenționale și neconvenționale la adresa securității naționale, de țări ostile și de organizații teroriste și criminale, de protecția fizică a demnitarilor și a obiectivelor strategice ale statului, precum și de protejarea informațiilor de stat clasificate. Caracterul secret dă serviciilor de informații un avantaj concurenţial în abordarea acestor preocupări, iar transparenţa extremă le-ar crea un dezavantaj evident şi periculos.

Mai precis, secretizarea e necesară pentru :

- a preveni cunoașterea de către țintele operațiunilor de informații a faptului că sunt puse sub urmărire;
- a preveni cunoașterea de către ținte și adversari a metodelor folosite de servicii;
- a proteja viața ofiţerilor de informaţii și a informatorilor;
- a apăra siguranța persoanelor foarte importante (VIP) care se află sub protecția serviciilor de informații;
- a păstra confidențialitatea informațiilor furnizate de serviciile străine de informații;
- a evita compromiterea pe diverse căi de către servicii rivale de informații.

În vreme ce aceste motive pentru secretizare sunt rezonabile, serviciile de informații tind spre o atitudine excesivă și, uneori, obsesivă privind secretizarea. Ele argumentează că transparența în zone care nu sunt sensibile va duce inexorabil spre deschidere în zonele sensibile, cu rezultate dramatice. În consecinţă, serviciile dezvoltă sisteme, proceduri și reguli interne care nu permit nicio relaxare sau flexibilitate în privința caracterului secret. În același timp, s-ar putea ca serviciile să preţuiască atât de mult secretizarea și fiindcă le oferă un anumit statut misterios, de elită.

Serviciile de informații sunt uneori reticente în a dezvălui informații chiar organismelor parlamentare de supraveghere care sunt autorizate să le primească. Serviciile își motivează reținerea prin aceea că parlamentarii nu au pregătirea și disciplina necesare pentru a păstra confidențialitatea și există riscul ca ei să divulge informații sensibile unor persoane neautorizate și să folosească greșit informațiile în scopuri politice partizane. Totuși, după cum se arată în continuare, pot fi aplicate o serie de măsuri care să minimizeze riscul de dezvăluire neautorizată a informațiilor.

2.2 SECRETIZAREA CA EXCEPȚIE, NU CA NORMĂ

Deoarece motivațiile de mai sus pentru secretizarea informațiilor sunt rezonabile, multe articole privind guvernanța democratică în domeniu afirmă că „trebuie găsit un echilibru adecvat între secretizare și transparență.” Însă, această formulă este prea neangajantă pentru a avea cât de cât valoare şi nu pleacă de la o premisă corectă. Punctul de plecare ar trebui să-l constituie principiile fundamentale ale democrației. Acestea includ transparența și dreptul persoanelor de a avea acces la informațiile deținute de stat. Sunt principii esențiale, deoarece reprezintă cerințe preliminare pentru: tragerea la răspundere a exe-

cutivului de către parlament și alte organisme de supraveghere; o supraveghere eficace din partea acestor organisme; libertatea politică și personală; contestarea democratică a puterii; dezbateri de substanță şi schimburi intense de idei; exercitarea deplină a calității de cetățean; și prevenirea abuzului de putere.

Ideea că libertatea informației este o bază necesară pentru alte drepturi și libertăți este cuprinsă în Rezoluția nr. 59(1) din 1946, a Adunării Generale a Națiunilor Unite, care proclamă că „libertatea informației este un drept fundamental al omului și temelia tuturor libertăților cărora le este consacrată Organizația Națiunilor Unite.” Aceeași logică se evidențiază în „Legea pentru promovarea accesului la informații,” adoptată în 2002 în Africa de Sud, care urmărește „să promoveze activ o societate în care populația Africii de Sud să aibă acces efectiv la informații, pentru a-i permite, în mai mare măsură, să-și exercite pe deplin toate drepturile și să le protejeze.”

Dat fiind că deschiderea e o condiție necesară pentru guvernanța democratică și protecția drepturilor omului, provocarea în sfera intelligence nu ar trebui definită ca „găsirea echilibrului corect între secretizare și transparență.” Mai curând, secretizarea ar trebui privită ca o *excepție care are nevoie*, *în fiecare caz, de o justificare convingătoare*. În vreme ce comunităţile de informaţii din întreaga lume, cu câteva excepţii, pun accentul pe secretizare, în societățile democratice, accentul ar trebui pus, cu unele excepții, pe deschidere. Este o chestiune atât de principiu, cât și de imperativ pragmatic. În istorie, există o mulțime de dovezi că probabilitatea abuzului de putere și a încălcării drepturilor omului este mai mare în condiții de secretizare decât într-un mediu politic deschis. Deschiderea permite o supraveghere eficace de către parlament și o examinare din partea mass-mediei și a grupurilor vigilente din societatea civilă, asigurând o bază pentru depistarea ilegalităților și a conduitei greșite și prevenind astfel apariția unei culturi a impunității.

2.3 RISCUL PRODUCERII UNUI PREJUDICIU PRECIZAT

Atunci, care este temeiul corect pentru stabilirea caracterului secret al informațiilor, ca o excepție în raport cu caracterul deschis? Răspunsul obișnuit în țările democratice și, deopotrivă, în cele cu regimuri autoritare, este „securitatea națională.” Ceea ce reprezintă o abordare eronată și primejdioasă din cauza elasticității și ambiguității conceptului de „securitate națională.”[2] Dacă securitatea națională este interpretată în sens larg, ca acoperind toate aspec-

[2] Pentru o discuție detaliată asupra acestui punct, a se vedea A. Wolfers, „National Security as an Ambiguous Symbol” [„Securitatea națională ca simbol ambiguu”], în *Political Science Quarterly* 67, no. 4 (1952), pp. 481–502.

tele securității umane, atunci secretizarea bazată pe acest teren vast poate duce la o clasificare excesivă și artificială a informațiilor. Chiar acolo unde „securitatea națională" are o definiție mai restrictivă, ea este invocată adeseori de stat pentru a justifica măsuri extraordinare, ce încalcă drepturile omului. De exemplu, oficialii de rang superior din Administrația SUA condusă de Președintele George W. Bush au aprobat utilizarea torturii în scopul protejării securității naționale.[3]

Într-o motivare din 1971, Curtea Supremă din SUA și-a exprimat preocuparea în privința impreciziei termenului de „securitate națională" în raport cu restrângerea libertății de exprimare:

> Cuvântul „securitate" este o noțiune generală amplă, imprecisă, ale cărei dimensiuni nu trebuie invocate pentru a abroga principiul fundamental consacrat de Primul Amendament (care se referă la libertatea de exprimare). Protejarea secretelor militare și diplomatice în detrimentul guvernării reprezentative, exercitate în cunoştinţă de cauză, nu oferă republicii noastre o securitate reală.[4]

Într-o democrație, termenul de „securitate națională" trebuie să acopere securitatea țării, a sistemului ei de guvernare, a valorilor ei și a tuturor persoanelor aflate sub jurisdicția statului respectiv. În consecință, el oferă un fundament care obligă mai curând la deschidere decât la secretizare. Nu este o noțiune de pus în balanță cu drepturile omului și libertățile individuale. O abordare democratică a securităţii naţionale include şi îşi însuşeşte drepturile omului şi libertăţile individuale.

În loc să se bazeze pe noțiunea amorfă de „securitate națională," secretizarea în comunitatea de informații trebuie motivată prin referirea la un *prejudiciu precizat și însemnat*, care ar putea decurge din dezvăluirea publică a unor informații. Ea ar trebui restrânsă la acele zone în care dezvăluirea publică ar produce un prejudiciu însemnat vieții unor persoane, serviciilor de informații, statului sau țării în ansamblu. Aceste zone cuprind următoarele:

- identitatea ofiţerilor de informaţii (alții decât șefii serviciilor de informații);
- identitatea informatorilor cu care lucrează serviciile de informații;
- detaliile tehnice ale metodelor operaționale;
- detaliile privind protecția persoanelor foarte importante (VIP);
- operațiunile și investigațiile în curs;

3 Uniunea Americană pentru Libertăți Civile, web site-ul *The Torture Report* (disponibil la www.thetorturereport.org).

4 *New York Times Co vs United States* [*New York Times Co versus Statele Unite*] 403 US 713 (1971) la 719.

- identitatea și datele personale ale indivizilor puși sub urmărire.

În funcție de circumstanțe, s-ar putea ca prejudiciul provocat de divulgarea informațiilor din zonele menționate mai sus să trebuiască a fi evaluat în raport cu intensitatea interesului public pentru dezvăluirea în cauză. Dezvăluirea în interes public ar putea fi o opțiune corectă dacă, de pildă, operațiunile de informații au avut drept ţintă, în mod ilegal, politicieni, dacă protecția acordată persoanelor foarte importante (VIP) este extrem de laxă, sau dacă ofiţeri de informaţii de rang superior au manifestat un comportament personal deosebit de compromițător. În general, guvernele democratice nu îşi pot propune să evite toate prejudiciile posibile care ar putea decurge din dezvăluirea publică a unor informații sensibile. Trebuie tolerat un oarecare nivel al prejudiciului, fiindcă pericolele atrase de secretizare pot amenința însăşi ordinea democratică.

Accesul public şi accesul liber al parlamentarilor la informaţii despre comunitatea de intelligence este necesarmente mai limitat decât accesul de care se bucură organismele specializate de supraveghere, precum o comisie parlamentară de supraveghere și un inspector general independent pentru informații. În vederea îndeplinirii mandatelor lor, aceste organisme au nevoie de mai multe informații decât cele disponibile în spaţiul public. Cerințele de informare ale organismelor respective sunt prezentate mai jos.

2.4 BENEFICIILE PRACTICE ALE CARACTERULUI DESCHIS AL INFORMAȚIILOR

Discuția precedentă s-a axat pe necesitatea unei deschideri în domeniul intelligence, din perspectiva guvernanței democratice, a respectului pentru drepturile omului și a prevenirii abuzului de putere. În plus, mai puţină secretizare și mai multă informaţie disponibilă privind serviciile de informații ar fi chiar în beneficiul serviciilor. Un sistem de clasificare care mărește excesiv volumul informațiilor clasificate e lipsit de credibilitate, e dificil de menținut și de pus în aplicare, e costisitor și ineficient. Se dedică prea mult timp și efort pentru clasificarea și protejarea unor informații inofensive, posibil în detrimentul apărării informațiilor cu adevărat sensibile.

În faimoasa decizie din 1971 a Curții Supreme din SUA, dată în cazul *Documente ale Pentagonului*, judecătorul Potter Stewart a afirmat următoarele în această privință:

> Atunci când totul e clasificat, nimic nu e clasificat, iar sistemul ajunge să fie ignorat de cei cinici sau indiferenţi și manipulat de cei care intenționează să se auto-protejeze ori auto-promoveze.[5]

În plus, după cum s-a remarcat în introducere, o mai mare transparență cu privire la serviciile de informații ar contribui la diminuarea suspiciunilor opiniei publice față de respectivele organizații și la creșterea încrederii publice în acestea. Ceea ce este vital într-o democrație, deoarece agențiile de informații trebuie să obțină informaţii de la indivizi și comunități mai curând prin relații de cooperare decât prin teroare şi coerciție.

3. LEGISLAȚIA PRIVIND PROTECȚIA INFORMAȚIILOR ȘI ACCESUL LA INFORMAŢII

În țările democratice, dezbaterea pe tema secretizării și transparenței informațiilor, evidenţiată mai sus, nu e niciodată rezolvată definitiv și permanent. Poate fi o arenă de luptă, în special în vremuri de criză și scandal în sfera intelligence, iar balanța poate înclina spre o deschidere mai mare sau spre o secretizare mai mare, în funcție de circumstanțele politice și de securitate ale țării, de conduita serviciilor de informații și de punctele de vedere ale executivului, parlamentului şi publicului.

Totuşi, în sens formal, dezbaterea e rezolvată cu ajutorul legislației care reglementează accesul la informațiile deținute de stat și protejarea acestora. De regulă, legislația respectivă include următoarele subiecte:

- principiile și criteriile pentru clasificarea și dezvăluirea informațiilor;
- autoritatea competentă şi procedurile de clasificare şi declasificare;
- verificarea de nivel înalt, judiciară sau de altă natură, a clasificărilor;
- dreptul persoanelor și al grupurilor de interes public de a obține acces la informațiile deținute de stat;
- procedurile pentru solicitarea unui astfel de acces și dreptul de apel dacă accesul e refuzat;
- rolul instanțelor în judecarea disputelor legate de clasificare și acces;
- pedepse pentru dezvăluirea ilegală de informații.

Serviciile de informații sunt, de regulă, responsabile pentru clasificarea informațiilor deținute de stat și pentru conceperea și menținerea sistemului de protejare a informațiilor clasificate. Ele ar putea fi implicate, de asemenea, în elaborarea proiectelor de lege aplicabile. De aici, pericolul ca legea să fie de-

---

5 *New York Times Co vs United States* [*New York Times Co versus Statele Unite*], 403 US 713 (1971).

turnată în favoarea unei secretizări excesive. Dat fiind că serviciile de informații au o tendinţă funcțională spre secretizare și împotriva deschiderii, responsabilitatea pentru elaborarea proiectelor de lege trebuie să revină ministerului de justiţie sau pentru probleme constituționale.

Parlamentul și comisiile sale de supraveghere, precum cele care se ocupă de chestiuni constituționale și de intelligence, au un rol crucial în a se asigura că legislația corespunde normelor democratice. Astfel de structuri pot ameliora calitatea și caracterul democratic al legii prin: solicitarea adresată executivului de a prezenta o motivare publică pentru legislația propusă și pentru orice prevederi controversate; facilitarea unor dezbateri de substanţă între partidele politice; organizarea de audieri publice care să permită cetăţenilor, mass-mediei și altor grupuri de interese să comenteze proiectele de lege; amendarea proiectelor de lege. În ultimă instanță, aprobarea legilor revine parlamentului.

În noile democrații, parlamentarii ar putea beneficia de pe urma unei examinări comparative internaționale în scopul stabilirii celor mai bune practici.[6] Următoarele aspecte pot fi considerate bune practici referitoare la legile care reglementează accesul la informații și protecția informațiilor:

- Legislația trebuie să recunoască explicit importanța transparenței și a accesului la informații ca principii fundamentale ale democrației, care promovează drepturile omului și libertățile individuale, buna guvernanță, răspunderea publică și dezbaterea informată. Legislația trebuie să stipuleze că clasificarea informațiilor este, în consecință, o măsură excepțională, care ar trebui folosită cu moderație.
- Legislația trebuie să urmărească, într-o manieră explicită, să prevină restricționarea nejustificată a accesului la informații (Caseta 1).
- Criteriile de clasificare a informațiilor trebuie să indice că s-ar putea produce, cu un anumit grad de certitudine, un prejudiciu însemnat în eventualitatea dezvăluirii lor publice. Legislația nu trebuie să permită recurgerea la secretizare pe baze nebuloase precum „securitatea națională” sau „interesul național.”
- Criteriile privind dezvăluirea sau nedezvăluirea informațiilor trebuie să fie precise și simple, pentru a facilita luarea unor decizii temeinice și consecvente de către oficialii guvernamentali și pentru a permite

[6] Ca exemplu pentru o astfel de analiză, a se vedea D. Banisar, „Public Oversight and National Security: Comparative Approaches to Freedom of Information” [„Supravegherea publică și securitatea națională: abordări comparative ale libertăţii de informare”], în *Democratic Control of Intelligence Services: Containing Rogue Elephants*, editori H. Born și M. Caparini (Aldershot, UK: Ashgate, 2007), pp. 217–235.

indivizilor să înțeleagă modul prin care își pot exercita dreptul de a obține informații deținute de stat.

- Legislația trebuie să prevadă evaluări ale situației informațiilor clasificate, la intervale specificate (de pildă, o dată la cinci ani), iar oficialii responsabili trebuie să informeze opinia publică asupra rezultatelor acestor evaluări.
- Atunci când se refuză cererea unei persoane pentru acces la informații deținute de stat, oficialul responsabil trebuie să-l informeze pe solicitant care este motivul pentru care informațiile respective nu pot fi dezvăluite și care este durata clasificării lor. Legea trebuie să prevadă că solicitantul, în temeiul unui interes personal sau public legitim, poate cere oficialului cu atribuții în domeniu să declasifice informațiile. Dacă acesta respinge cererea, solicitantul trebuie să aibă dreptul de a ataca decizia în justiţie. Apelul trebuie examinat de un judecător.
- Legislația trebuie să prevadă mai degrabă clasificarea *informațiilor* decât clasificarea *documentelor*. În acest fel, oficialii guvernamentali vor avea posibilitatea să clasifice informațiile sensibile dintr-un document fără a fi nevoie să clasifice întregul document. Asemenea documente pot fi apoi dezvăluite public într-o formă editată.
- Atunci când informațiile clasificate sunt relevante pentru procedurile din instanță, decizia privind examinarea informațiilor cu ușile închise sau în ședință publică trebuie să revină mai curând judecătorului decât executivului.
- Legislația trebuie să permită persoanei acuzate de dezvăluirea ilegală a unor informații clasificate să invoce în apărarea sa divulgarea „în interes public." Această situație poate să survină atunci când, de exemplu, un ziar divulgă detalii despre instalarea ilegală a unor microfoane de către serviciile de informații. Validitatea apărării din raţiuni de interes public trebuie apreciată de judecătorul care examinează cazul.
- Legislația trebuie să impună executivului obligația de a promova și facilita accesul public la informațiile deținute de stat, inclusiv, după cum se arată mai jos, la datele privind serviciile de informații.

Această listă a elementelor de legislație ce constituie o bună practică are de-a face în egală măsură cu chestiuni procedurale și cu chestiuni de substanță și se referă la informațiile deținute de stat care includ – dar nu se limitează la – informaţii privind comunitatea de informații. Următoarele secțiuni se axează pe

aspectele de fond din domeniul intelligence, care ar trebui să fie puse la dispoziția diferitelor organisme de supraveghere.

Caseta 1: Evitarea clasificării necorespunzătoare a informațiilor

Decretul prezidențial din SUA referitor la clasificare stabilește că informațiile nu pot fi clasificate cu scopul de a ascunde încălcări ale legii, ineficiență ori erori administrative; de a preveni punerea într-o situație delicată a unei persoane, organizații sau agenții; ori de a împiedica sau amâna dezvăluirea unor informații care nu necesită protecție în interesul securității naționale. În mod asemănător, „Legea privind protecția informațiilor clasificate" din Slovenia interzice clasificarea informațiilor referitoare la infracțiuni. În Mexic și Peru, legislația aferentă împiedică clasificarea informațiilor legate de încălcarea drepturilor omului și a normelor de drept internațional.[7]

4. INFORMAŢIILE NECESARE PARLAMENTULUI

Într-o democrație, parlamentul este principala instituție responsabilă pentru supravegherea activităților executivului și ale departamentelor de stat. Pentru a îndeplini această responsabilitate în ceea ce privește comunitatea de informații, parlamentul trebuie informat cu privire la: prioritățile din domeniul intelligence; politici, reglementări și acțiuni ale executivului în domeniul intelligence; evaluări, bugete și rapoarte financiare din domeniul intelligence; rapoartele SAI privind serviciile de informații; activitățile și constatările organismelor specializate de supraveghere a serviciilor de informații; orice investigații asupra conduitei serviciilor de informații. Această secțiune analizează informațiile de care are nevoie parlamentul, reunit în plen, în ședință cu caracter public, în contrapondere cu informațiile de care au nevoie comisiile parlamentare de supraveghere a serviciilor de informații, despre care se va vorbi mai târziu.

4.1 PRIORITĂȚILE NAȚIONALE ÎN DOMENIUL INTELLIGENCE

Din când în când, de regulă anual, executivul trebuie să decidă care vor fi prioritățile sale în domeniul intelligence pentru perioada următoare. Și asta, fiindcă serviciile de informații nu trebuie să își traseze ele însele sarcinile, iar stabilirea priorităților în raport cu amenințările și zonele de acțiune constituie o chestiune de politică de înalt nivel. Prin determinarea de către executiv a priorităților în domeniu, se stabilește orientarea politică a serviciilor și se pun

7 Informațiile din această casetă sunt extrase din Banisar, „Public Oversight" [„Supravegherea publică"].

bazele pentru planificare, bugetare, alocarea resurselor, operațiuni și pentru stabilirea responsabilităţilor.

Prioritățile naționale ale executivului în domeniul intelligence (NIP) nu trebuie să fie clasificate. Discuțiile parlamentare asupra NIP sunt de natură să întărească responsabilitatea, precum și caracterul democratic al procesului decizional în raport cu un aspect al politicii naționale care are o influență profundă asupra siguranței și bunăstării persoanelor aflate sub jurisdicția statului respectiv. Securitatea națională nu ar fi subminată prin dezvăluire, deoarece NIP pot fi furnizate parlamentului fără a numi indivizi sau organizații anume, făcând în schimb referire la categorii precum „crimă organizată," „terorism" și „proliferare nucleară."

Informațiile sensibile ar putea fi eliminate din versiunea NIP care e prezentată parlamentului și ar putea fi furnizate confidențial comisiei parlamentare de supraveghere a serviciilor de informații.

4.2 POLITICILE, REGLEMENTĂRILE ȘI ACȚIUNILE EXECUTIVULUI

Politicile și reglementările executivului în domeniul intelligence sunt frecvent secrete chiar în democrațiile bine consolidate. Fapt anormal și de nedorit, deoarece încalcă principiul cardinal al responsabilității. Regulile principale care guvernează serviciile de informații, îndeosebi cele referitoare la metodele de investigare care încalcă drepturile constituționale, ar trebui să fie supuse dezbaterii și revizuirii de către parlament. E necesar să se facă o distincție între regulile și procedurile departamentale care trebuie ținute secret, fiindcă dezvăluie detalii tehnice sensibile ale metodelor operaționale, și reglementările și politicile executivului care trebuie să fie de domeniu public, deoarece sunt parte integrantă a guvernanței democratice.

În temeiul legislației privind domeniul intelligence, executivul trebuie să prezinte parlamentului, spre analiză și comentarii, politicile și reglementările sale asupra următoarelor aspecte:

- exercitarea funcțiilor și puterilor de către organizațiile de informații, inclusiv a puterilor lor de a încălca drepturile constituționale;
- politicile operaționale, excluzând detaliile tehnice sensibile;
- controlul ministerial și relația dintre serviciile de informații și șeful statului, cabinet și ministrul cu responsabilități în domeniu;
- relația dintre diferitele servicii de informații și repartizarea responsabilităților între acestea, coordonarea activităților în domeniu și funcțiile fiecărui mecanism naţional de coordonare în materie;

- relațiile cu serviciile străine de informații; criteriile și regulile pentru schimbul de informații cu guverne străine referitor la persoane;
- sistemul disciplinar al serviciilor de informații și mecanismele interne prin care se asigură respectarea constituției și a statului de drept.

Parlamentul răspunde pentru supravegherea executivului și a instituțiilor de stat. În consecință, el are nevoie să fie informat despre acțiunile semnificative ale guvernului în privința serviciilor de informații. Acțiunile relevante includ numirea și demiterea staffului de rang înalt; acțiunea disciplinară împotriva staffului de rang înalt; autorizarea ministerială a operațiunilor intruzive, acolo unde aceasta e cerută prin lege (a se vedea Hutton – Instrumentul 5); și reformele și inovările majore din sistemele și operațiunile comunității de informații. Informațiile prea sensibile pentru domeniul public trebuie să fie prezentate comisiei parlamentare de supraveghere a serviciilor de informații.

4.3 RAPOARTELE ANUALE ALE SERVICIILOR DE INFORMAȚII

Într-o democrație, publicarea unor rapoarte anuale de către departamentele guvernului și alte organe ale statului este un mijloc necesar de asigurare a responsabilității față de parlament și opinia publică în general. Ea oferă parlamentului o bază pentru a stabili dacă prioritățile și politicile guvernului sunt însușite și dacă banii contribuabililor sunt cheltuiți eficient. Nu există niciun motiv valabil pentru ca serviciile de informații să fie excluse din această practică. Rapoartele anuale ale Serviciului General de Informații și Securitate din Olanda (AIVD) oferă un exemplu excelent de furnizare a unor informații cuprinzătoare și utile, fără a compromite securitatea națională.[8]

Rapoartele anuale ale serviciului de informații trebuie să acopere următoarele chestiuni (fără a divulga detaliile sensibile): obiectivele și prioritățile anuale ale serviciului; evaluarea sa în privința amenințărilor majore la adresa securității; orice reforme majore în politicile, sistemele și operațiunile serviciului de informații; îndeplinirea, de către serviciu, a funcțiilor sale de raportare și asumare a răspunderii; și răspunsul acestuia la cererile de informare în temeiul legislației privind libertatea informației.

[8] Aceste rapoarte pot fi găsite pe web site-ul Serviciului General de Informații și Securitate din Olanda (disponibil la https://www.aivd.nl/english/). Pentru raportul din 2010, a se vedea https://www.aivd.nl/english/publications-press/@2827/annual-report-2010.

4.4 EVALUĂRILE SERVICIILOR DE INFORMAȚII

În multe situații, evaluările făcute de comunitatea de informații, referitoare la indivizi și organizații, nu se pretează a fi prezentate parlamentului din cauza riscului de compromitere a unor operațiuni de informații și a unor cercetări penale. Cu toate acestea, evaluările făcute de serviciile de informații referitoare la tipuri de securitate și de amenințări la adresa securității pot fi, în multe cazuri, comunicate public, fără a exista riscul vreunui prejudiciu.

Ca exemplu, Serviciul Canadian pentru Informații de Securitate (CSIS) publică o serie de materiale ce cuprind: documente de suport pe teme precum securitatea economică, proliferarea armelor și lupta împotriva terorismului; o publicație intitulată *Commentary* [„Comentariu”], care se axează pe chestiuni legate de securitatea Canadei; și o serie de rapoarte de cercetare, bazate pe analiza CSIS a unor informații din surse deschise.[9] Rapoartele anuale ale Serviciului General de Informații și Securitate din Olanda merg până acolo, încât includ comentarii despre organizațiile radicale și teroriste, menționându-le numele.[10]

Prezentarea unor astfel de evaluări parlamentului și comisiei/comisiilor sale de supraveghere a serviciilor de informații e o formă importantă de responsabilizare, care permite parlamentarilor, teoreticienilor și organizațiilor neguvernamentale să discute despre abordările serviciilor de informaţii în materie de politici şi de securitate. În timp, discuțiile bine fundamentate, parlamentare și publice, pot conduce la o rafinare a acestor abordări.

4.5 BUGETELE, RAPOARTELE FINANCIARE ȘI RAPOARTELE INSTITUȚIILOR SUPREME DE AUDIT

În țările democratice, parlamentul primește, examinează și dezbate bugetele anuale și rapoartele financiare ale organismelor guvernamentale. Este o formă indispensabilă de responsabilizare, ce permite reprezentanților aleși ai poporului să supravegheze și să aprobe utilizarea fondurilor publice în conformitate cu legislația, politica guvernului și propriile priorități și opțiuni ale parlamentului. Totuși, versiunile complete ale rapoartelor financiare și ale bugetelor serviciilor de informații sunt, de regulă, prezentate cu titlu confidențial numai comisiei parlamentare de supraveghere și nu sunt înaintate parlamentului în ansamblu (a se vedea Wills – Instrumentul 8).

---

[9] A se vedea web site-ul Serviciului Canadian pentru Informații de Securitate, disponibil la www.csis-scrs.gc.ca.

[10] A se vedea Banisar, „Public Oversight” [„Supravegherea publică”].

Caseta 2: Publicarea bugetelor și a rapoartelor financiare ale serviciilor de informaţii

În 2006, Comisia ministerială de verificare a serviciilor de informaţii din Africa de Sud a examinat bugetele, rapoartele financiare și planurile strategice clasificate, prezentate anual de serviciile de informații comisiei parlamentare de supraveghere a serviciilor de informații. Comisia a ajuns la concluzia că publicarea acestor documente nu ar compromite în niciun fel operațiunile serviciilor de informații ori securitatea țării. Comisia a fost de acord cu opinia Trezoreriei Naționale că bugetele și rapoartele financiare ale serviciilor de informaţii ar trebui prezentate în mod deschis parlamentului. Detaliile sensibile ar putea fi incluse doar în documentele care sunt analizate în ședințele cu ușile închise ale comisiei de supraveghere.[11]

Organizațiile de informații se opun dezvăluirii bugetelor lor pe motivul că serviciile străine de informații ar obţine astfel un avantaj asupra lor. Este un argument exagerat. Un serviciu străin de informații nu va avea niciun beneficiu dacă va cunoaşte cât cheltuie o altă ţară pentru serviciile ei de informaţii. Și nici nu va apărea vreun avantaj ori prejudiciu din dezvăluirea modului în care îşi repartizează fondurile pentru cheltuielile de personal, costuri de funcţionare și cheltuieli de capital. Numai la un nivel mult mai înalt al detaliilor – în ceea ce privește țintele, metodele, sursele, rezultatele și constrângerile operaționale – securitatea ar putea fi subminată prin dezvăluire (a se vedea Caseta 2).

Caseta 3: Protecția informațiilor sensibile în auditul financiar

„Legea auditului public” (2004) din Africa de Sud conține mai multe prevederi legate de protecția informațiilor sensibile. Ea stipulează că auditorul general trebuie să ia măsuri de precauție pentru a preveni dezvăluirea informațiilor secrete sau clasificate, obținute pe parcursul unui audit. Atunci când raportează despre un cont confidențial de securitate, auditorul general „trebuie să acorde atenția cuvenită naturii speciale a contului și, la recomandarea scrisă a ministrului relevant, în temeiul interesului național, poate exclude detaliile confidențiale, secrete sau clasificate ale constatărilor din raportul de audit, cu condiția ca raportul de audit să menţioneze că aceste detalii au fost excluse.”

11 Africa de Sud, Comisia ministerială de verificare a serviciilor de informaţii, *Intelligence in a Constitutional Democracy: Final Report to the Minister for Intelligence Services, the Honourable Mr. Ronnie Kasrils, MP* [*Intelligence într-o democrație constituțională: Raport final în atenția ministrului pentru serviciile de informații, Hon. Mr. Ronnie Kasrils, MP*] (10 septembrie 2008) (disponibil la www.ssronline.org/document_result.cfm?id=3852).

Într-o manieră similară, un raport anual al SAI referitor la serviciile de informații ar trebui să aibă două versiuni: un raport public ce e prezentat parlamentului și un raport clasificat, conținând mai multe detalii, care e prezentat comisiei parlamentare de supraveghere cu atribuții în domeniu. Legislația care reglementează rapoartele auditorului general trebuie să asigure protecția informațiilor sensibile (a se vedea Caseta 3).

4.6 GESTIONAREA SCANDALURILOR DIN DOMENIUL INTELLIGENCE

Discuția precedentă s-a axat pe informaţiile de care are nevoie parlamentul, în mod firesc, în vederea îndeplinirii responsabilității sale de supraveghere. Dacă există o criză ce implică serviciile de informații (de exemplu, dezvăluirea unor acțiuni de spionare a politicienilor), parlamentul poate înființa o comisie de anchetă sau poate cere unuia dintre organismele specializate de supraveghere a serviciilor de informaţii să facă o investigaţie. Constatările investigației trebuie să fie prezentate parlamentului și dezbătute cu ușile deschise. Dacă nu se va proceda astfel, opinia publică nu va avea nicio încredere în investigaţie și nici siguranța că eventualul delict a fost tratat corespunzător.

5. INFORMAȚIILE NECESARE ORGANISMELOR SPECIALIZATE DE SUPRAVEGHERE A SERVICIILOR DE INFORMAȚII

Informaţiile de care au nevoie organismele specializate de supraveghere a serviciilor de informaţii – dintre care, în primul rând comisia parlamentară de profil, un inspector general independent pentru informații și un organism specializat de supraveghere a serviciilor de informații (precum Comisia de Verificare a Serviciilor de Informații și de Securitate din Olanda) – derivă din mandatul și funcțiile acestor organisme. Mandatul și funcțiile diferă de la o țară la alta, însă pot include următoarele:

- respectarea de către serviciile de informaţii a constituției, legislației, reglementărilor, precum și a politicilor guvernului;
- performanţele și succesul serviciilor de informații în raport cu mandatul şi funcţiile lor stabilite prin lege și cu prioritățile determinate de guvern;
- sistemele și metodele interne de prevenire, depistare și gestionare a conduitei incorecte;
- sistemele financiare interne și cheltuielile.

Din perspectiva acestor funcții de supraveghere, secțiunea de față analizează necesităţile în materie de informare ale unei comisii parlamentare de supraveghere a serviciilor de informații, ale unui inspector general pentru informații și

ale altor instituții de tip ombudsman, precum și ale puterii judecătoreşti. Secțiunea analizează apoi căi de minimizare a riscului de dezvăluire involuntară sau deliberată a informațiilor clasificate.

5.1 COMISIILE PARLAMENTARE DE SUPRAVEGHERE A SERVICIILOR DE INFORMAŢII

Comisia parlamentară de supraveghere a serviciilor de informaţii ar trebui să primească, în mod firesc, toate informaţiile în domeniu, care sunt prezentate parlamentului în ansamblul său. Comisia, de regulă, ar trebui să fie prima care primeşte aceste informații, astfel încât, înainte de dezbaterea parlamentară, să aibă ocazia de a le examina cu atenție, de a delibera asupra lor și a interacționa cu ofiţerii de informaţii de rang superior și cu membrul/membrii din executiv cu responsabilităţi în materie. Comisia, în mod colectiv, și membrii săi, care reprezintă diferite partide politice, sunt astfel pregătiţi să aibă contribuţii bine fundamentate într-o dezbatere parlamentară mai amplă.

În plus, comisia de supraveghere trebuie să primească pe cale confidențială informații mai detaliate și mai sensibile decât cele care sunt prezentate întregului parlament. Subiectele asupra cărora trebuie să primească informații detaliate includ următoarele:

- prioritățile naționale ale executivului în domeniul intelligence;
- politicile, reglementările și acțiunile executivului în domeniul intelligence;
- rapoartele anuale ale serviciilor de informații;
- evaluările făcute de servicii în privința securității și amenințărilor;
- bugetele și rapoartele financiare anuale ale serviciilor;
- rapoartele SAI asupra serviciilor;
- activitățile și constatările organismelor specializate de supraveghere a serviciilor de informații (dacă există).

Chestiunea crucială și dificilă este aceea de a determina cât de multe detalii și ce nivel de sensibilitate ar trebui să aibă informaţiile prezentate comisiei de supraveghere. Pe de o parte, membrii comisiei nu sunt instruiți în ceea ce priveşte păstrarea caracterului secret și, inevitabil, ei au loialităţi politice mixte, atât față de țara lor, cât și față de partidul politic din care fac parte. Mai mult, există axioma potrivit căreia cu cât este mai mare numărul oamenilor care dețin o informație secretă, cu atât mai mică va fi probabilitatea ca ea să rămână secretă. Prin urmare, serviciile de informații sunt reticente în a dezvălui detalii sensibile privind operațiunile, metodele și personalul lor. Pe de altă parte, comisia parlamentară trebuie să primească îndeajuns de multe

informații detaliate pentru a-și desfășura supravegherea în mod corespunzător. Dacă sunt prea multe informații care nu parvin membrilor comisiei, supravegherea va fi superficială și nu va depista sau examina corespunzător o conduită greșită, rezultatele slabe sau o utilizare defectuoasă a fondurilor.

Chestiunea legată de numărul detaliilor şi nivelul de sensibilitate al informaţiilor ce trebuie prezentate comisiei parlamentare de supraveghere se impune a fi abordată în cadrul legislației, cât mai precis posibil, cu scopul de a minimiza posibilitatea apariției unor neînțelegeri și dispute între parlament și serviciile de informații și/sau ramura executivă. Modul în care asemenea reguli și linii directoare sunt formulate în legislație diferă de la o țară la alta (a se vedea mai multe exemple în Caseta 4).

Caseta 4: Prevederi legislative referitoare la accesul la informații al comisiilor parlamentare de supraveghere

În România, serviciile de informații sunt obligate să dea curs, într-o perioadă rezonabilă de timp, solicitărilor de informaţii primite din partea comisiei parlamentare de supraveghere în domeniu, cu excepția cazului în care, procedând astfel, ar periclita operaţiunile în curs, identitatea agenţilor, metodele sau sursele. Comisiile parlamentare pot face vizite neanunțate serviciilor și trebuie să li se acorde acces deplin la personal, date și facilități.[12] Prin contrast, în Marea Britanie, mandatul actual al comisiei parlamentare de supraveghere este limitat la „cheltuielile, administrarea și politicile" serviciilor de informații și de securitate, fiind implicit excluse operațiunile din sfera de acţiune a comisiei și limitându-se, astfel, accesul ei la informații.[13]

Legislația trebuie să specifice totodată mijloacele de soluționare a disputelor privind accesul comisiei parlamentare la informații. În Africa de Sud, de pildă, legea în materie stabilește că disputele vor fi rezolvate de o comisie *ad hoc* din care fac parte ministrul pentru domeniul intelligence, șeful serviciului de

12 C. Matei, „Romania's Transition to Democracy and the Role of the Press in Intelligence Reform" [„Tranziția României spre democrație și rolul presei în reforma domeniului intelligence"], în *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness*, editori T. Bruneau și S. Boraz (Austin: University of Texas Press, 2007), p. 227.

13 P. Gill, „Evaluating Intelligence Oversight Commitees: The UK Intelligence and Security Commitee and the 'War on Terror'" [„Evaluarea comisiilor de supraveghere a serviciilor de informaţii: Comisia britanică pentru informații și securitate și «Războiul împotriva terorii»"], în *Intelligence and National Security* 22, no. 1 (februarie 2007), pp. 14–37.

informații, președintele comisiei parlamentare de supraveghere și inspectorul general pentru informații.[14]

Puterile comisiei parlamentare de supraveghere de a obține informaţii din domeniul intelligence diferă de la o țară la alta. În mod obişnuit, comisia trebuie să primească rapoarte regulate de la membrul/ membrii executivului cu responsabilităţi în domeniu, de la serviciile de informații, SAI, judecătorul sau membrul din executiv responsabil pentru autorizarea operațiunilor intruzive, precum și de la toate organismele specializate de supraveghere a serviciilor de informații. De asemenea, comisia trebuie să fie împuternicită să solicite un raport din partea oricăreia din entitățile amintite. În plus, ea poate avea competența de a efectua o anchetă, de a cita martori și de a inspecta incintele serviciilor de informații.

5.2 INSPECTORII GENERALI PENTRU INFORMAȚII ȘI ALTE INSTITUȚII DE TIP OMBUDSMAN

Caracterul secret care înconjoară serviciile de informații face ca o supraveghere eficace să întâmpine dificultăți substanțiale. În consecință, este nevoie de organisme de supraveghere a acestor servicii, care să dispună de competențe speciale și de expertiza unor specialiști. Un astfel de organism este un inspector general (IG) independent pentru informații.[15] Pentru a desfășura o supraveghere eficace într-un mediu secret, Inspectorul General (IG) trebuie să aibă următoarele atribute:

- IG trebuie să fie un oficial independent, care să aibă siguranța menţinerii în funcţia respectivă.
- El/ea trebuie să aibă mandatul și competențele legale pentru a monitoriza respectarea de către servicii a constituției, legislației și a politicilor guvernului, precum și pentru a investiga reclamațiile de conduită incorectă, ilegalitate și abuz de putere.
- IG trebuie să raporteze nu numai ministrului cu responsabilităţi în domeniu, ci și comisiei parlamentare de supraveghere a serviciilor de informaţii, iar, în cazul unor investigații majore, și parlamentului în ansamblul său.

[14] Africa de Sud, Intelligence Services Oversight Act [Lege privind supravegherea serviciilor de informații], Legea nr. 40 din 1994, Secțiunea 4(2)(b).

[15] Trebuie făcută distincţia între un inspector general pentru informații, ca poziție independentă cu statut propriu (precum în Australia, Noua Zeelandă și Africa de Sud) și poziţia din cadrul unei organizații de informații (precum Agenția Centrală de Informații din SUA).

- IG și stafful său trebuie să aibă un înalt nivel de expertiză și experiență în domeniul intelligence.

În plus, legislația care reglementează un astfel de organism, trebuie să prevadă că inspectorului general și staffului său nu li se poate refuza accesul la informații, date sau incinte aflate sub controlul serviciilor de informații și că orice refuz al unui asemenea acces constituie o infracțiune. Acestea sunt cerințe esențiale atunci când un organism de supraveghere independent investighează operațiuni și sisteme secrete.

Comentariile precedente despre IG se aplică în egală măsură și altor instituții de tip ombudsman, așa cum sunt comisarii pentru drepturile omului în țările în care nu există un inspector general pentru informații. Marele avantaj în utilizarea unui IG specializat constă în faptul că inspectorul general și stafful său dispun de expertiză în domeniul intelligence, ceea ce îi ajută atât să depisteze faptele reprobabile comise într-un mediu secret, cât şi să protejeze corespunzător informaţiile clasificate la care au acces.

La auditarea cheltuielilor, alocărilor bugetare, veniturilor (dacă există) și sistemelor financiare ale serviciilor de informații, SAI trebuie să aibă acces la toate informațiile referitoare la operațiunile și fondurile secrete ale serviciilor (pentru mai multe detalii, a se vedea Wills – Instrumentul 8). Prin urmare, SAI trebuie să aibă o echipă de specialiști care au fost instruiți să gestioneze documente clasificate și au primit certificatul de securitate. Ca alternativă, ar putea fi potrivit ca oficiul inspectorului general independent pentru informații să efectueze auditul financiar în cooperare cu SAI.

5.3 PUTEREA JUDECĂTOREASCĂ

Serviciile de informații și agențiile de aplicare a legii încalcă dreptul la viață privată atunci când desfășoară operațiuni intruzive, precum interceptarea comunicațiilor, perchezițiile și sechestrarea. În consecință, în majoritatea țărilor democratice, organismele guvernamentale trebuie să obțină o autorizație judiciară pentru a întreprinde astfel de operațiuni (pentru alte detalii, a se vedea Hutton – Instrumentul 5). În funcție de țară, agențiile pot apela la orice judecător în acest scop sau poate exista un judecător special desemnat, care examinează toate cererile de interceptare.

Informațiile de care are nevoie un judecător sunt precizate, de regulă, în legislația privind interceptarea comunicațiilor. Solicitantul trebuie să furnizeze suficiente fapte care să-l convingă pe judecător că interceptarea e un mijloc necesar și justificabil pentru culegerea de informații despre o activitate criminală sau o amenințare la adresa securității naționale ori a siguranței publice. S-ar putea ca legislația să considere interceptarea comunicațiilor ca o metodă la

care să se recurgă în ultimă instanță, în care caz, solicitantul trebuie să îl convingă pe judecător şi de faptul că metodele neintruzive sunt inadecvate sau necorespunzătoare.

Pe lângă chestiunea cererilor de interceptare, cazurile penale sau civile care privesc comunitatea de informații pot fi examinate în instanță dacă, de exemplu, un ofiţer de informaţii este acuzat de o infracțiune sau dacă un politician afirmă că în biroul său au fost instalate ilegal microfoane. S-ar putea ca executivul să vrea ca unele sau toate cazurile de acest gen să fie audiate cu ușile închise. Democrațiile diferă în ceea ce privește modul în care este abordată această problemă. Chestiunea poate fi tranșată cu ajutorul legislației sau poate fi lăsată la discreția judecătorului care prezidează (Caseta 5).

Caseta 5: Gestionarea informațiilor sensibile în cadrul procedurilor din instanță

Într-un caz examinat de Curtea Constituțională din Africa de Sud în 2008, un grup de ziare a cerut un ordin pentru a obliga la dezvăluirea publică a unor porţiuni restricționate din înregistrarea procedurilor judiciare care au implicat Agenția Națională de Informații (NIA). Grupul și-a întemeiat cererea pe dreptul la o justiţie transparentă. Ministrul pentru informații s-a opus dezvăluirii, invocând raţiuni de securitate naţională. Curtea a decis dezvăluirea unei părți a materialului, considerând că nu există nici un temei valid de natura securităţii naţionale, care să împiedice dezvăluirea, însă a apreciat că celelalte informaţii – privind relațiile cu serviciile străine de informații, ierarhia de comandă în cadrul NIA și identitatea agenților NIA – trebuie să rămână restricționate. În opinia unei minorități s-a considerat că dezvăluirea întregului material, cu excepția numelui anumitor agenți, era în interesul public.[16]

5.4 CREȘTEREA RĂSPUNDERII ORGANISMELOR DE SUPRAVEGHERE

Țările democratice pot avea o supraveghere parlamentară sau independentă relativ puternică a serviciilor de informații și, totuși, este posibil ca răspunderea organismelor de supraveghere faţă de populaţie să nu fie adecvată. Organismele de supraveghere sunt ele însele prea secretoase. Ceea ce subminează încrederea publică atât în aceste organisme, cât și în serviciile de informații. Le revine, deci, organismelor de supraveghere sarcina să prezinte parlamentului rapoarte elocvente și să publice pe website-ul lor propriile rapoarte, precum și

---

[16] *Independent Newspapers (Pty) Ltd vs Minister for Intelligence Services* [*Independent Newspapers (Pty) Ltd versus ministrul pentru serviciile de informații*] CCT 38/07 [2008] ZACC 6 (Africa de Sud).

rapoarte ale serviciilor de informații. Un bun exemplu pentru o astfel de practică este Comisia de Verificare a Serviciilor de Informații și de Securitate din Olanda, care publică anual un raport cuprinzător asupra monitorizării și investigațiilor pe care le-a efectuat.[17]

5.5 MINIMIZAREA RISCULUI DE DEZVĂLUIRE A INFORMAȚIILOR CLASIFICATE

După cum s-a arătat mai înainte, serviciile de informații sunt uneori reticente în ceea ce privește dezvăluirea informațiilor sensibile către comisiile parlamentare de supraveghere, deoarece membrii celor din urmă sunt politicieni și, de obicei, nu au instruirea necesară în materie de disciplină și practici de protejare a informațiilor clasificate. Ca urmare, există riscul de dezvăluire, deliberată sau involuntară, a unor informații sensibile. Pentru minimizarea unui asemenea risc, pot fi luate următoarele măsuri:

- Legislația privind protecția informațiilor trebuie să stipuleze că dezvăluirea neautorizată a unor informații clasificate constituie o infracțiune.
- Membrii comisiilor parlamentare de supraveghere trebuie să fie supuși verificării de către un serviciu de informații înainte de numirea lor în astfel de comisii.[18]
- Comisiile trebuie să fie împuternicite prin lege să ţină şedinţe cu ușile închise.
- Experții din domeniul intelligence trebuie să se asigure că birourile comisiilor de supraveghere, computerele, telefoanele și sistemele de evidenţă sunt protejate împotriva urmăririi.
- Experții din domeniul intelligence trebuie să asigure formarea şi instruirea membrilor şi staffului comisiilor.
- Comisiile și serviciile de informații trebuie să convină asupra regulilor şi procedurilor referitoare la primirea, deţinerea, utilizarea și distrugerea informațiilor clasificate.

Măsurile menționate mai sus sunt relevante, în întregime sau parțial, și pentru alte organisme specializate de supraveghere. Totuși, dat fiind că aceste orga-

---

[17] Rapoartele anuale ale acestei comisii pot fi consultate la http://www.ctivd.nl/.

[18] Pentru mai multe informații privind verificarea membrilor comisiilor parlamentare de supraveghere, a se vedea H. Born și I. Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* [*Responsabilizarea în domeniul intelligence: standarde legale și cele mai bune practici pentru supravegherea agențiilor de informații*] (Geneva: DCAF, Universitatea din Durham și Parlamentul Norvegiei, 2005), pp. 88–90.

nisme sunt formate din profesioniști, în contrast cu politicienii, e posibil ca riscul dezvăluirii unor informaţii clasificate să fie mai mic.

6. RECOMANDĂRI

- Transparența și accesul la informațiile deținute de stat sunt condiții necesare pentru guvernanța democratică, protecția drepturilor omului și prevenirea abuzului de putere. Prin urmare, secretizarea ar trebui să constituie o excepție. În ceea ce privește comunitatea de informații, secretizarea trebuie motivată printr-un prejudiciu precizat şi semnificativ care ar putea să se producă în urma dezvăluirii de informații. Ea ar trebui limitată la acele aspecte a căror dezvăluire ar periclita în mod serios viaţa unor persoane, serviciile de informaţii, statul sau ţara în ansamblul ei. Prejudiciul cauzat de dezvăluire ar trebui pus în balanță cu interesul public ce obligă la dezvăluire.
- Responsabilitatea pentru elaborarea legislaţiei referitoare la protecția informațiilor și accesul la informaţii trebuie să revină departamentului de justiție sau pentru probleme constituționale, și nu serviciilor de informații. Prin strădania lui, parlamentul trebuie să se asigure că legislația este compatibilă cu normele democratice.
- Legislația trebuie să sublinieze că transparența și accesul la informații sunt principii fundamentale ale democrației, iar secretizarea informațiilor trebuie utilizată cu moderație. Criteriile de clasificare trebuie să indice un nivel îndeajuns de ridicat al prejudiciului și certitudinea că nedivulgarea este garantată. Legislația trebuie să permită unei persoane acuzate de dezvăluirea ilegală a unor informații clasificate să-și întemeieze apărarea pe motivul rațiunilor de interes public. Executivul trebuie să fie obligat să promoveze și să faciliteze accesul public la informațiile deținute de stat, inclusiv la cele referitoare la serviciile de informații.
- Parlamentul trebuie informat cu privire la: prioritățile din domeniul intelligence; politicile, reglementările și acțiunile în materie ale executivului; evaluările, bugetele și rapoartele financiare din domeniul intelligence; rapoartele SAI cu privire la serviciile de informații; activitățile și constatările organismelor specializate de supraveghere a respectivelor servicii; și orice investigații asupra conduitei serviciilor de informații. Comisia parlamentară de supraveghere a serviciilor de informații trebuie să primească în mod confidențial informații mai detaliate și mai sensibile cu privire la subiectele de mai sus. Informațiile trebuie să fie suficiente comisiei pentru a-și îndeplini într-o manieră corespunzătoare funcțiile de supraveghere. Detaliile în acest sens trebuie specificate în legislație.

- Legislația referitoare la inspectorul general pentru informații și/sau la organismul specializat de supraveghere a serviciilor de informații trebuie să prevadă că nu se poate refuza accesul entității și al staffului său la informații, date sau incinte aflate sub controlul serviciilor de informații și că orice refuz de acest fel constituie o infracțiune.
- În cazurile penale sau civile care implică serviciile de informații, decizia de a examina cazurile respective parțial sau integral cu ușile închise trebuie luată de judecătorul care prezidează.
- Organismele de supraveghere trebuie să prezinte parlamentului rapoarte și să publice pe website-ul lor propriile rapoarte, precum și rapoarte ale serviciilor de informații.
- Pot fi luate măsuri pentru reducerea riscului ca membrii comisiei parlamentare de supraveghere a serviciilor de informaţii să divulge, deliberat sau involuntar, informații clasificate: membrii săi pot fi verificați de un serviciu de informații; ei pot fi instruiți în vederea protejării informațiilor clasificate; iar birourile, computerele, telefoanele și sistemele de evidenţă pot fi protejate împotriva urmăririi.

INSTRUMENTUL 4

Efectuarea supravegherii

Monica den Boer



4

Efectuarea supravegherii

Monica den Boer

1. INTRODUCERE

În noile democrații, supravegherea eficace a comunității de informații este crucială din cauza tensiunii inerente care există între munca în domeniul intelligence și anumite valori democratice, cum sunt deschiderea și transparența. Dacă serviciile naționale de informații trebuie să fie puse sub un control extern civil, atunci civilii trebuie să acumuleze cunoştinţe despre munca de informații. Altminteri, această activitate va continua să fie monopolizată de profesioniștii serviciului. De asemenea, trebuie să se dezvolte o nouă cultură politică în măsură să prevină abuzurile, continuând, în acelaşi timp, să susţină rolul legitim al serviciilor de informații într-o societate democratică.

Acest instrument explică modul în care organismele de supraveghere investighează serviciile de informații. El analizează cea mai amplă gamă posibil de tipuri de supraveghere, pornind de la investigațiile *ad hoc* și mergând până la anchetele pe termen lung. În plus, sunt analizate acele situații în care mai multe organisme permanente au responsabilități de supraveghere, precum și situaţiile în care nu există niciun organism permanent, ceea ce impune crearea unui organism temporar.

Mai mult, se intenționează ca acest instrument să servească drept ghid practic pentru modul în care se efectuează supravegherea serviciilor de informații. Dat fiind că organismele de supraveghere din diferite țări se confruntă cu multe provocări similare, înțelegerea metodologiei de bază poate ajuta organismele de profil nou create să evite capcanele și să-și maximizeze eficacitatea.

2. MOTIVE PENTRU EFECTUAREA SUPRAVEGHERII SERVICIILOR DE INFORMAŢII

Responsabilitatea în domeniul intelligence are mai multe niveluri. Unele se referă la controlul serviciilor de informații practicat pe plan intern de oficialii din cadrul acestora, iar pe plan extern, de membri ai executivului. Altele se referă la supravegherea exercitată de parlament, de puterea judecătorească și de organismele specializate de supraveghere (a se vedea Born și Geisler Mesevage – Instrumentul 1). Scopul fundamental al supravegherii serviciilor de informaţii este acela de a descuraja o activitate necorespunzătoare din partea serviciilor naționale de informații. Prin opoziție cu *controlul*, care se referă la conducerea directă a serviciului, *supravegherea* include monitorizarea, evaluarea, examinarea și verificarea. Prin promovarea deschiderii și transparenței, organismele de supraveghere pot restrânge tendințele abuzive din cadrul unui serviciu și pot oferi membrilor parlamentului și executivului (și altor entităţi care exercită responsabilități de control) informații utile și expertiză.

2.1 ÎNCĂLCAREA DREPTURILOR OMULUI

Posibila încălcare a drepturilor omului de către serviciile de informații constituie întotdeauna un motiv de îngrijorare publică. În deceniile ’60-’70, de exemplu, agențiile guvernamentale din SUA au autorizat operațiuni de intelligence sub acoperire, cu caracter agresiv, care s-au îndreptat împotriva drepturilor civile și mișcărilor antirăzboinice. Mai recent, serviciile naționale de informații, în cadrul cooperării pentru combaterea terorismului, au folosit practici precum extrădarea extraordinară, funcționarea centrelor secrete de detenție și utilizarea de informații obținute prin tortură. Aceste practici care amenință fățiș drepturile omului sunt, toate, subiecte adecvate pentru supraveghere.

Activitățile necorespunzătoare și/sau ilegale sunt deseori aduse în atenția organismelor de supraveghere de către mass-media, în special de jurnaliștii de investigații, care acționează pe baza indiciilor primite de la organizații neguvernamentale cum sunt Human Rights Watch și Amnesty International. Conform spuselor Marinei Caparini,

> Mass-media constituie o reţea care conectează indivizi și grupuri cu guvernul și care are un rol esenţial în transmiterea informațiilor despre schimbările la nivelul opiniei publice şi al preferinţelor politice … Populația poate fi informată în primul rând prin intermediul unei prese libere, iar guvernul poate fi tras la răs-

pundere prin intermediul ameninţării cu examinarea publică a deciziilor și acțiunilor sale, precum și a abuzurilor de putere săvârșite.[1]

2.2 ÎNTREBĂRI PARLAMENTARE

Membrii parlamentelor naționale, chiar cei care nu fac parte din comisiile de supraveghere, pot pune întrebări despre activitățile serviciilor de informații. Acestea pot varia de la întrebări generale despre nivelul amenințărilor și prioritățile serviciilor, până la întrebări precise despre metodele folosite în operațiunile sub acoperire și interacțiunile cu anumite grupuri. Uneori, întrebările pot identifica un vid în legislație, ce apare atunci când e inițiată o nouă operațiune pentru care nu există încă un mecanism de supraveghere. De pildă, în 2003, parlamentarii olandezi au pus întrebări despre modul de culegere a informațiilor privind alegațiile despre armele de distrugere în masă deținute de fostul guvern al lui Saddam Hussein în Irak.[2] Aceste întrebări au dus la înființarea în Olanda a Comisiei de anchetă referitoare la Irak.

3. MANDATE DE SUPRAVEGHERE

Serviciile de informații trebuie să se conformeze legilor, directivelor, mandatelor și politicilor guvernelor pe care le servesc.[3] În mod asemănător, organismele de supraveghere a serviciilor de informaţii trebuie să respecte legile sau mandatele prin care sunt stabilite, dar și limitate, competențele lor de investigare. Mandatele de supraveghere sunt redactate, de obicei, în forma cea mai neutră posibil, în ideea de a evita controversele politice. Ceea ce este deosebit de important atunci când organismul de supraveghere e temporar, ca în cazul anchetării pe baze *ad hoc* a unui anumit incident. Totuși, mandatele trebuie să fie precise, clare și proporționale cu puterile, metodele și resursele pe care le are/au serviciul/serviciile de supravegheat.

Mandatele organismelor de supraveghere pot fi complementare sau se pot suprapune. Ultima variantă e de preferat, deoarece un singur mecanism de supraveghere e considerat, în general, insuficient. Din acest motiv, în Italia, sistemul de supraveghere a serviciilor de informații a fost de curând extins de la o simplă supraveghere *ex post*, efectuată de Curtea Constituțională, și a inclus

1 Marina Caparini, "Controlling and Overseeing Intelligence Services in Democratic States" [„Controlul și supravegherea serviciilor de informații în statele democratice"], în *Democratic Control of Intelligence Services:Containing Rogue Elephants*, editori: Hans Born și Marina Caparini (Aldershot, UK: Ashgate, 2007), p. 12.

2 Comisia pentru afaceri externe, 26 septembrie 2003, 03-BuZa-61.

3 În interesul legitimității sociale, serviciile de informații trebuie să acționeze și în conformitate cu interesul public. Și anume, trebuie să se abțină de la a invada fără temei viața privată a cetățenilor, într-o manieră disproporționată și/sau ilegală.

două noi mecanisme: un organism administrativ intern (Biroul Inspectorului General) și un mecanism politic extern (Comisia parlamentară pentru securitatea Republicii – COPASIR).[4] În ceea ce privește Serviciul Canadian pentru Informații de Securitate (CSIS) există patru mecanisme de supraveghere care se suprapun: un Inspector General, care monitorizează conformitatea activităţilor CSIS cu politicile operaţionale; o Comisie de Verificare a Informațiilor de Securitate (SIRC), care verifică activitățile CSIS și investighează reclamațiile împotriva serviciului (a se vedea Farson – Instrumentul 2); Curtea Federală a Canadei, care e singurul organism autorizat să permită utilizarea măsurilor speciale de investigare; [5] și raportarea publică sub forma Declarației anuale a ministrului pentru siguranța publică cu privire la securitatea naţională şi Raportul public al CSIS.[6]

Mandatul unei comisii parlamentare de supraveghere, precum COPASIR, trebuie să acopere întreaga comunitate națională de informaţii, inclusiv departamentele și oficialii care o sprijină.[7] Mandatul trebuie să confere comisiei întreaga autoritate de care are nevoie pentru a monitoriza legalitatea, eficacitatea și eficiența serviciilor de informații, precum și practicile lor de bugetare și de evidență contabilă, respectarea standardelor în materia drepturilor omului și alte aspecte legate de politici/administrare. Dacă nu reușește să îndeplinească aceste obiective, mandatul comisiei trebuie revizuit. De exemplu, atunci când, într-o anchetă *ad hoc* din Australia, s-a constatat că Organizația de Imagistică și Informații Geospațiale pentru Apărare (DIGO) nu avea un grad de răspundere îndeajuns de mare, din cauza unui mandat de supraveghere limitat, ancheta a recomandat ca mandatul comisiei parlamentare de supraveghere cu atribuţii în domeniu să fie extins pentru a include toate serviciile de informații din Australia. Ancheta a mai recomandat ca mandatul Inspectorului

---

4 Tommaso F. Giupponi și Federico Fabbrini, „Intelligence agencies and the State secret privilege: the Italian Experience" [„Agențiile de informații și privilegiul secretului de stat: experiența italiană"], în *International Constitutional Law Journal* 4, no. 3 (toamna anului 2010), pp. 443–466 (disponibil la http://www.internationalconstitutionallaw.net/download/53c4319b67f44d52a392c655f17245a3/Giupponi_Fabbrini.pdf).

5 Măsurile speciale de investigare includ interceptarea comunicațiilor, coordonarea informatorilor și a persoanelor infiltrate și construirea aparențelor.

6 Website-ul Serviciului Canadian pentru Informații de Securitate, „Accountability and Review" [„Responsabilitate și verificare"] (disponibil la http://www.csis-scrs.gc.ca/bts/ccntblt-eng.asp).

7 În general, se recomandă ca întreaga comunitate de informații a unei națiuni să fie supusă supravegherii efectuate de cel puțin o comisie parlamentară.

General pentru Informații și Securitate să fie extins pentru a include monitorizarea DIGO (a se vedea Born și Geisler Mesevage – Instrumentul 1).[8]

3.1 TIPURI DE MANDATE

Mandatele pot fi ample sau restrânse. De pildă, mandatul unui organism de supraveghere poate fi pur și simplu acela de a verifica legalitatea activităților unui singur serviciu de informații. Un alt organism poate fi însărcinat să verifice eficacitatea mai multor agenții, inclusiv performanţele cadrelor de conducere și derularea procesului bugetar. Mandatele mai ample contribuie, în general, la evitarea unei supravegheri fragmentate sau imperfecte din alte puncte de vedere.

Uneori, mandatele de supraveghere includ competențe care se extind dincolo de ceea ce este strict necesar pentru realizarea monitorizării. De exemplu, pot include puterea de a aresta și de a plasa în detenţie preventivă, precum și de a utiliza forţa letală. De asemenea, pot include controlul transferului de informații către servicii străine și aprobarea numirilor făcute de executiv în funcţiile cele mai înalte din domeniul intelligence.[9]

În ceea ce privește activitățile sub acoperire, în special acolo unde sunt utilizate măsuri de investigare pentru culegerea datelor cu caracter personal, mandatele includ uneori puteri preventive sau proactive. De pildă, în Belgia, „Legea privind informațiile speciale” autorizează Comisia Permanentă pentru Verificarea Agențiilor de Informații (Comisia I – un organism specializat de supraveghere) să dea un aviz serviciilor de informații în privința utilizării măsurilor speciale de investigare. Dacă avizul este negativ, serviciile nu îl pot contesta. Mai mult, dacă pe parcursul monitorizării modului de utilizare a măsurilor speciale de investigare, Comisia permanentă identifică practici ilegale, ea le poate suspenda.[10]

---

8 Website-ul Departamentului australian al Primului ministru și al Cabinetului: *Report of the Inquiry into Australian Intelligence Agencies*, Chapter 4 [*Raportul anchetei cu privire la agențiile australiene de informații*, Capitolul 4] (disponibil la www.dpmc.gov.au/publications/intelligence_inquiry/chapter4/oversight.htm).

9 Hans Born, „Towards Effective Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practice” [„Către o supraveghere democratică efectivă a serviciilor de informații: lecții învățate din compararea practicilor naționale”], în *Connections: Quarterly Journal* 3, no. 4 (decembrie 2004), p. 6 (disponibil la http://www.pfpconsortium.org/file/1645/view).

10 Guy Rapaille, „Le Comité permanent R dans un rôle d’organe juridictionnel: Le nouveau rôle du Comité belge dans le cadre du contrôle des methodes particulières de recueil de données” [„Comitetul permanent R în rolul unui organ jurisdicțional: noul rol al Comitetului belgian în cadrul controlului asupra metodelor speciale de

Mandatele de supraveghere pot include și verificări de natură bugetară. De exemplu, în Marea Britanie, auditul contabilității serviciului de informații este efectuat de Oficiul Național de Audit, iar Comisia parlamentară pentru informații și securitate examinează și ea același subiect, căci, în raportul ei anual, face publice unele detalii privind finanţarea şi cheltuielile serviciului.[11] Într-o manieră similară, în Africa de Sud, Comisia mixtă pentru informații examinează managementul financiar al serviciilor naţionale de informații; [12] în același timp, în Polonia, comisia parlamentară de supraveghere verifică proiectele de buget din domeniul intelligence și monitorizează implementarea lor. Unele state merg atât de departe, încât includ controlul bugetar în mandatele organismelor lor de supraveghere. De pildă, Comisia bicamerală pentru supravegherea organismelor și activităților de informații din Argentina și comisiile pentru informații din Congresul SUA dispun de această competență.

3.2 SCHIMBĂRI ÎN MANDATE

Mandatele organismelor de supraveghere a serviciilor de informaţii nu trebuie să fie fixe. De pildă, atunci când mandatul unui serviciu de informații se extinde, mandatul organismului care îi supraveghează activitățile trebuie să fie, de asemenea, revizuit.[13]

Evenimentele strategice cu repercusiuni politice semnificative pot, de asemenea, să producă schimbări în mandatele organismelor de supraveghere a serviciilor de informaţii, în special atunci când respectivele evenimente implică

culegere a datelor”] (expunere la cea de-a 6-a Conferință a comisiilor parlamentare pentru supravegherea serviciilor de informații și securitate din statele membre ale Uniunii Europene, Bruxelles, 30 septembrie – 1 octombrie 2010) (disponibil la http://www.parlement-eu2010.be/pdf/30sep-1okt-Thema0-Guy-Rapaille.pdf).

[11] De exemplu, a se vedea Marea Britanie, Comisia pentru informații și securitate, *Annual Report 2010–2011*, Cm 8114 (2011) [*Raport anual 2010–2011*, Cm 8114 (2011)] (disponibil la http://www.cabinetoffice.gov.uk/sites/default/files/resources/isc-annualreport1011.pdf).

[12] Sandy Africa, „The South African Intelligence Services: A Historical Perspective” [„Serviciile de informații din Africa de Sud: o perspectivă istorică”], în *Changing Intelligence Dynamics in Africa*, editori: S. Africa și J. Kwadjo (Birmingham, UK: Global Facilitation Network for Security Sector Reform/African Security Network, 2009), pp. 61–94.

[13] Pentru o discuție asupra acestui punct, a se vedea Paul Robinson, *Eyes on the Spies: Reforming Intelligence Oversight in Canada* [*Cu ochii pe spioni: reforma supravegherii serviciilor de informații în Canada*], Centre for International Policy Studies (CIPS) Document orientativ nr. 1 (Ottawa: CIPS, University of Ottawa, noiembrie 2008) (disponibil la http://www.sciencessociales.uottawa.ca/cepi-cips/eng/documents/CIPS_PolicyBrief_Robinson_Nov2008.pdf).

eșecuri ale acestor servicii. De exemplu, eșecul comunității de informații din SUA în detectarea și prevenirea atacurilor din 11 septembrie 2001 au dus la reconsiderarea mecanismelor de comunicare a informațiilor. Schimbările aduse acestor mecanisme au avut un impact asupra muncii organismelor de supraveghere, impunând și o schimbare în mandatele lor.

Alteori, organismele de supraveghere, pe parcursul activității lor, identifică ele însele modificări pe care este nevoie să le facă în propriile mandate. Din acest motiv, unele organisme de supraveghere efectuează în mod regulat examinări de ordin strategic, pentru a identifica și recomanda asemenea schimbări. Astfel, organismele de supraveghere pot transforma deficiențele în recomandări constructive, pozitive, în scopul perfecționării activității din sectorul intelligence.

4. COMPETENȚE DE SUPRAVEGHERE

Competențele conferite organismelor de supraveghere variază foarte mult. Cele descrise mai jos fac parte dintre cele mai obișnuite. Însă lista nu e completă. De exemplu, unele mandate includ puterea de sesizare, care autorizează un organism de supraveghere să sesizeze o conduită incorectă unui organism intern (așa cum e un inspector general) în vederea aplicării unor măsuri disciplinare, sau unui organism extern în vederea declanșării urmăririi penale. Competența de denunţare dă organismelor de supraveghere puterea de a informa cea mai înaltă autoritate a statului respectiv, așa cum este Procurorul General din SUA, despre situații de nerespectare a legii, erori de judecată sau încălcări ale legii; este o competență ce depășește cu mult sesizarea unui inspector general.

4.1 DREPTUL LA INFORMAȚIE

Dreptul la informație, care dă organismelor de supraveghere acces la informații, poate fi pasiv sau activ. Un organism de supraveghere cu drept la informație pasiv poate primi informaţii despre activitățile din domeniul intelligence sub forma unui document și prin intermediul unor briefinguri. În mod ideal, aceste briefinguri au loc în mod curent şi sunt cuprinzătoare; însă, în funcție de legile aplicabile, ele nu pot include informații cu grad mare de sensibilitate, așa cum sunt chestiunile bugetare și operațiunile sub acoperire.

Organismele de supraveghere care dispun numai de drept la informație pasiv sunt dependente în totalitate de agențiile pe care le supraveghează în privința anvergurii și preciziei informațiilor pe care le primesc. Din acest motiv, e de preferat ca organismele de supraveghere să dispună atât de dreptul la informație pasiv, cât și de cel activ. Organismele de supraveghere cu drept la

informație activ sunt împuternicite să caute informațiile de care au nevoie – de exemplu, obligând oficialii să le furnizeze informații sau efectuând vizite neanunțate în incinta serviciului în cauză.

Deși organismele de supraveghere ar trebui să aibă acces nelimitat la toate informațiile care le sunt necesare pentru a-şi îndeplini îndatoririle, nu se întâmplă întotdeauna astfel. De pildă, accesul la informații clasificate îl au majoritatea organismelor de supraveghere, dar nu toate. Pe de altă parte, unele restricții pot fi impuse din prudență, aşa cum sunt cele care protejează identitatea surselor. Astfel de restricții se aplică, de exemplu, pentru accesul la informații al Comisiei parlamentare mixte permanente pentru informații din Africa de Sud. În Argentina, Canada și SUA, anumite organisme de supraveghere au acces nelimitat la informații.

4.2 COMPETENȚE DE INVESTIGARE

Pe lângă simpla capacitate de a examina informațiile ce le-au fost furnizate, organismele de supraveghere a serviciilor de informaţii au nevoie de puterea de a iniția investigații. Comisia olandeză de Verificare a Serviciilor de Informații și de Securitate (CTIVD), de pildă, are puterea de a iniția investigații pe baza reclamațiilor pe care le primește împotriva serviciilor de informații. Mandatele altor organisme de supraveghere le autorizează să inițieze investigații din proprie iniţiativă, fără a se baza pe o reclamație. Puterile specifice de investigare cuprind autoritatea de a cere oficialilor și/sau a-i obliga să se prezinte în fața organismului respectiv de supraveghere pentru a răspunde la întrebări.

4.3 COMPETENȚE DE APROBARE

Unele mandate dau organismelor de supraveghere dreptul de a aproba sau de a autoriza programe strategice în domeniul intelligence, bugetul serviciilor și/sau numirile la cel mai înalt nivel. Organismele de supraveghere care dețin una sau mai multe dintre aceste competențe de aprobare le pot folosi pentru a exercita o influență semnificativă asupra serviciilor pe care le supraveghează, îndeosebi în ceea ce priveşte stabilirea priorităților în activitatea de intelligence. De exemplu, „puterea portmoneului,” exercitată de comisiile pentru informații din Congresul SUA, este considerată un instrument puternic de supraveghere și control, deoarece permite comisiilor să indice prioritățile în materie de intelligence și politici prin intermediul alocărilor bugetare.

5. METODE DE SUPRAVEGHERE

Pe lângă precizarea atribuțiilor, mandatul unui organism de supraveghere trebuie să definească metodele pe care acesta le poate utiliza în desfășurarea

unei investigații. Cel mai frecvent folosite sunt inspecțiile, audierile și analiza documentelor. Alte metode includ interviurile, declarațiile martorilor și accesul direct la baze de date (ultima dintre ele fiind considerată de oficialii belgieni și olandezi ca o metodă-cheie de supraveghere). Toate metodele sunt utilizate în mod individual, în tandem şi secvențial, pentru atingerea scopurilor supravegherii.

5.1 INSPECȚIILE

Unele organisme de supraveghere efectuează inspecții regulate în incintele serviciilor de informații pe care le supraveghează. Aceste vizite pot avea loc anual, trimestrial sau chiar lunar. În majoritatea cazurilor, organismele de supraveghere aduc la cunoștința serviciilor de informații vizitele pe care urmează să le facă, însă multe dintre ele sunt autorizate să facă inspecții neanunțate. În timpul vizitelor, membrii organismului de supraveghere pot intervieva angajații sau pot examina bazele de date computerizate folosind tehnici precum sondajele aleatorii. În Norvegia, comisia parlamentară de supraveghere a serviciilor de informații (cunoscută drept Comisia EOS) efectuează mai multe inspecții în fiecare an; în Olanda, CTIVD are un mandat similar. În Noua Zeelandă, Inspectorul General pentru Informații și Securitate are autoritatea de a intra în incinta serviciilor, dar numai dacă directorul serviciului în cauză a fost notificat în prealabil.[14]

5.2 AUDIERI

Audierile sunt o modalitate obișnuită prin care organismele de supraveghere obțin informații din partea oficialilor din serviciile de informaţii, a experților independenți și a altor respondenți. Cu toate că sunt laborioase și sensibile, audierile pot fi esențiale în reconstituirea unei situații despre care înregistrările documentare nu oferă suficiente date sau care a fost tăinuită. Audierile pot contribui și la stabilirea responsabilităților politice și/ori executive pentru decizii luate și/sau implementate de serviciile de informații și alți oficiali. Ancheta în curs din Marea Britanie asupra implicării naționale în războiul din Irak, prezidată de Sir John Chilcot, a inclus numeroase audieri, toate fiind difuzate în timp real.[15] Comisia olandeză de anchetă referitoare la Irak a organizat audieri asemănătoare, care, însă, nu au fost publice.

---

[14] Comisia de anchetă privind acțiunile oficialilor canadieni în cazul Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* [*Un nou mecanism de verificare a activităților RCMP legate de securitatea națională*] (2006), p. 351 (disponibil la http://www.sirc-csars.gc.ca/pdfs/cm_arar_rcmpgrc-eng.pdf).

[15] Website-ul Anchetei Irak, „About the Inquiry" [„Despre anchetă"] (disponibil la http://www.iraqinquiry.org.uk/about.aspx).

5.3 ANALIZA DOCUMENTELOR

Organismele de supraveghere verifică cu regularitate rapoartele clasificate și neclasificate, precum și alte documente prezentate de serviciile de informații. Aceste documente furnizează deseori informații utile și pot răspunde unor întrebări; în același timp, însă, ele pot ridica alte întrebări legate de munca serviciilor de informații, cărora trebuie să li se răspundă pe alte căi.

Analiza documentelor nu trebuie limitată la materialele prezentate de serviciile de informații. Comisia olandeză de anchetă referitoare la Irak, de exemplu, a creat un website public pentru a solicita alte documente care ar putea fi utile.

6. PROGRAMAREA SUPRAVEGHERII

Supravegherea poate avea loc înainte de luarea unei decizii în privința unei operațiuni sau politici, în timpul implementării sau după implementare. Programarea supravegherii depinde de mandatul organismului de supraveghere (a se vedea Born și Geisler Mesevage – Instrumentul 1).

6.1 SUPRAVEGHEREA *EX POST*

Cea mai comună formă de supraveghere este supravegherea *ex post*. Rațiunea fundamentală este aceea că organismele de supraveghere trebuie să verifice deciziile de management ale serviciilor de informații, dar să nu interfereze cu ele.[16] Supravegherea *ex post* nu exclude, în mod necesar, încunoștințarea organismelor de supraveghere în privința operațiunilor planificate sau în curs de realizare, dar ea pune un accent puternic pe abordarea retrospectivă a evenimentelor, examinându-se doar evenimentele care deja s-au petrecut.

6.2 SUPRAVEGHEREA *EX ANTE*

Unele organisme de supraveghere au mandatul de a efectua supravegherea *ex ante*. Aceasta e privită ca un mijloc de a întări autoritatea sistemului de supraveghere. Ea implică inspecția și/sau aprobarea activităților de intelligence înainte de a fi inițiate. Se poate vorbi și despre un „mandat proactiv," care e definit ca „un mandat care permite organismului de supraveghere să interzică sau

---

[16] Pentru o discuție privind sistemul norvegian de supraveghere a serviciilor de informații, care are această abordare, a se vedea Trygve Harvold, „Norwegian Parliamentary Oversight: an ‚effective remedy'?" [„Supravegherea parlamentară din Norvegia: un «remediu efectiv»?"] (expunere la cea de-a 6-a Conferință a comisiilor parlamentare pentru supravegherea serviciilor de informații și securitate din statele membre ale Uniunii Europene, Bruxelles, 30 septembrie – 1 octombrie 2010) (disponibil la www.parlement-eu2010.be/pdf/30sep-1okt-Thema-Trygve Harvold.pdf).

să modifice politica sau funcționarea serviciilor înainte ca politica sau operațiunea în cauză să fie puse în practică.”[17] Numeroase organisme de supraveghere sunt în situația de a examina strategia și politicile serviciilor de informații relevante și pot cere sau indica organismelor de verificare interne să efectueze o investigație înainte de demararea unei activităţi specifice sau a unei operaţiuni de intelligence sub acoperire.

Raportorul special al Națiunilor Unite pentru promovarea și protejarea drepturilor omului și libertăților fundamentale în contextul combaterii terorismului recomandă supravegherea *ex ante*, pe care o consideră utilă pentru prevenirea încălcării drepturilor omului de către serviciile de informații în lupta împotriva terorismului. În mod similar, se recomandă ca organismele de supraveghere să efectueze verificarea *ex ante* a acordurilor de cooperare între serviciile naționale de informații și partenerii străini înainte de semnarea acestora (a se vedea Roach – Instrumentul 7).[18]

Pe de altă parte, organismele de supraveghere care efectuează verificarea *ex ante* pot fi trase la răspundere pentru eșecuri și încălcări ale legii în sfera intelligence, care se produc ca rezultat al activităților aprobate. Totodată, abilitarea unui organism de supraveghere de a efectua o verificare *ex ante* poate bloca relațiile cu parteneri străini care preferă să nu dezvăluie informaţii confidenţiale organismelor de supraveghere.[19]

Multe dintre serviciile interne de informații manifestă îngrijorări similare în privința securității atunci când e vorba de dezvăluirea în avans a informațiilor legate de operațiuni, în special când sunt implicaţi parlamentari. Din acest mo-

---

[17] Hans Born, „Towards Effective Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practice” [„Către o supraveghere democratică efectivă a serviciilor de informații: lecții învățate din compararea practicilor naționale”], în *Connections: The Quarterly Journal* 3, no. 4 (decembrie 2004), p. 9 (disponibil la http://www.pfpconsortium.org/file/1645/view).

[18] Consiliul Națiunilor Unite pentru Drepturile Omului, *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development: Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, [*Promovarea și protejarea tuturor drepturilor omului, a drepturilor civile, politice, economice, sociale și culturale, inclusiv dreptul la dezvoltare: Raportul Raportorului special al Națiunilor Unite pentru promovarea și protejarea drepturilor omului și libertăților fundamentale în contextul combaterii terorismului*], Document al Națiunilor Unite A/HRC/10/3 (4 februarie 2009), p. 24 (disponibil la http://www.unhcr.org/refworld/pdfid/49b138c32.pdf).

[19] Born, „Towards Effective Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practice.”

tiv, deseori, parlamentarii care fac parte din comisiile de supraveghere a serviciilor de informații trebuie să treacă prin verificarea de securitate. Uneori, nici chiar această măsură de precauție nu e considerată suficientă.

6.3 SUPRAVEGHEREA PERIODICĂ

Supravegherea poate avea loc şi periodic. În mod frecvent, mandatele serviciilor de informații impun conducerii lor superioare să pregătească rapoarte periodice (de regulă, anuale) cu privire la activităţile serviciilor, pentru a fi prezentate executivului, parlamentului sau amândurora. De asemenea, și organismele de supraveghere pot să-și efectueze examinarea mai curând ciclic decât ocazional. Recunoscându-și capacitatea limitată, SIRC din Canada a adoptat un plan care asigură supravegherea tuturor aspectelor referitoare la serviciile de informații într-un ciclu de trei până la cinci ani. Raportul anchetei australiene *ad hoc* asupra serviciilor de informații (despre care s-a discutat mai înainte) a recomandat, în mod similar, ca verificările asupra comunității de informații să aibă loc o dată la cinci până la șapte ani.[20]

7. INVESTIGAȚIILE ÎN CADRUL SUPRAVEGHERII

În cadrul supravegherii, investigațiile pot fi inițiate pe mai multe căi diferite. Parlamentarii sau executivul le pot solicita oficial. Mass-media poate crea agitație în favoarea lor. În unele țări, precum Belgia și Canada, reclamația făcută de un cetățean oarecare va atrage după sine o investigaţie. Adeseori, organismele de supraveghere sunt împuternicite să inițieze propriile lor investigații. Totuși, în cele mai multe cazuri, organismele de supraveghere își rezervă decizia finală cu privire la problemele de care se vor ocupa sau nu.

7.1 INVESTIGAREA UNOR CAZURI SPECIFICE

Organismele de supraveghere pot iniția investigații asupra unor cazuri specifice în temeiul alegațiilor făcute, de pildă, de reclamanți, de parlamentari sau de mass-media. Se pot desfășura investigații asupra anumitor evenimente sau alegații privind serviciile de informații, şi aceste investigații pot fi inițiate chiar de organismele de supraveghere. În funcție de procedurile corespunzătoare, serviciile de informații pot furniza organismului de supraveghere rapoarte asupra unor incidente serioase, care se pot referi, de exemplu, la activități ilegale, breșe de securitate sau scurgeri de informații. Aceste rapoarte pot fi fur-

[20] Website-ul Departamentului australian al Primului ministru și al Cabinetului: *Report of the Inquiry into Australian Intelligence Agencies* [*Raportul anchetei cu privire la agențiile australiene de informații*], Capitolul 8, Recomandarea 22 (disponibil la www.dpmc.gov.au/publications/intelligence_inquiry/chapter8/1_findings.htm).

nizate fie regulat, fie cu ocazia anchetelor *ad hoc*. Un astfel de raport a fost pregătit de Poliția Regală Călare din Canada (RCMP) pentru Comisia de anchetă privind acțiunile oficialilor canadieni în cazul Maher Arar. Printre altele, ancheta a stabilit că RCMP nu și-a respectat propriile politici ce impun examinarea riguroasă a datelor cu caracter personal, pentru a stabili dacă sunt relevante şi sigure, înainte de a le transmite altor servicii de informații. Printre cele 23 de recomandări ale comisiei se afla și avertismentul ca RCMP să rămână în limitele mandatului său ca forță de poliție.[21]

7.2 INVESTIGAȚII TEMATICE

Investigațiile tematice se axează în principal pe chestiuni generale şi mai puţin pe anumite evenimente. Uneori, ele au ca punct de pornire anchete privind evenimente specifice, ale căror constatări evidențiază chestiuni de mult mai mare anvergură.

8. ORGANIZAREA SUPRAVEGHERII

Dat fiind că cea mai eficace supraveghere e cea sistematică, este instructiv să separăm procesul de supraveghere în etape distincte, succesive.

8.1 IDENTIFICAREA ȘI SELECTAREA PROBLEMELOR

Munca de informații este un domeniu complex, dinamic, ce implică numeroși actori și mai multe proceduri și politici. Din acest motiv, o gamă largă de probleme pot deveni subiecte ale unei supravegheri. Cea mai bună modalitate de a începe un proces de supraveghere este alcătuirea unui inventar al tuturor problemelor posibile și compararea lui cu mandatul legal al organismului de supraveghere. Problemele care se regăsesc atât în inventar, cât și în mandat constituie subiecte potrivite pentru examinare.

8.2 OBȚINEREA CERTIFICATULUI DE SECURITATE

Membrii și angajații organismelor de supraveghere trebuie, de regulă, să obțină certificate de securitate în vederea lucrului cu informații clasificate. Excepții notabile sunt membrii comisiilor parlamentare de supraveghere, care au tendința de a refuza investigarea vieții lor personale, în special atunci când serviciul de informații care efectuează verificarea este, paradoxal, chiar entita-

[21] Comisia de anchetă privind acțiunile oficialilor canadieni în cazul Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* [*Raportul evenimentelor legate de cazul Maher Arar: analiză și recomandări*] (2006), Capitolul 9 (disponibil la http://www.sirc-csars.gc.ca/pdfs/cm_arar_rec-eng.pdf).

tea supusă verificării sau investigării. Cu toate acestea, exceptarea politicienilor de la verificarea de securitate este puternic controversată.

8.3 SECURIZAREA BIROULUI ORGANISMULUI DE SUPRAVEGHERE

Biroul organismului de supraveghere trebuie să fie securizat. De pildă, el trebuie verificat periodic pentru înlăturarea dispozitivelor electronice de urmărire. În plus, computerele și celelalte echipamente informatice trebuie să fie parolate și criptate. În mod asemănător, tot personalul de suport care are acces în incintă (inclusiv secretare, translatori, personal de catering, personal de curățenie) trebuie să treacă printr-un control de securitate.

Caseta 1: Ancheta parlamentară olandeză asupra măsurilor speciale de investigare: studiu de caz privind supravegherea tematică

În 1993, o echipă interregională olandeză pentru investigații penale, căreia i s-a trasat sarcina de a culege informații despre un traficant de droguri, a folosit măsuri speciale de investigare pentru a-și îndeplini îndatoririle. După cum s-a pretins, aceste măsuri au inclus acte ilegale, îndeosebi eliberarea controlată de droguri pe piață. Ca reacție la aceste alegații de conduită incorectă, echipa a fost dizolvată, iar, în aprilie 1994, parlamentul olandez a inițiat o anchetă oficială asupra utilizării măsurilor speciale de investigare de către autoritățile olandeze.[22]

Ancheta a început cu analiza documentelor și convorbiri orientative cu politicieni și profesioniști din domeniul intelligence. În plus, ancheta a delegat unor specialişti din mediul universitar sarcina de a pregăti două rapoarte: o evaluare a naturii, gravității și amplorii crimei organizate în Olanda și un studiu internațional comparativ al legislației ce reglementează utilizarea măsurilor speciale de investigare.

În același timp, stafful implicat în desfășurarea anchetei (supus în ansamblu verificării de securitate) a ținut audieri cu ușile închise vreme de șase luni. Scopul audierilor a fost obţinerea de informații despre utilizarea măsurilor speciale de investigare în Olanda și înțelegerea lor temeinică. Audierile cu ușile închise au servit, de asemenea, la pregătirea unei serii de audieri deschise, publice, care au fost difuzate în direct.

În urma anchetei, care s-a încheiat în 1996, a fost elaborat un raport detaliat de 6.700 de pagini, ce cuprindea 129 de recomandări. Doi ani mai târziu, parlamentul a înființat o nouă comisie, temporară, pentru analizarea gradului de aplicare a acelor recomandări. Noua comisie a adus multe informații noi, inclusiv probe privind corupția legată de droguri în cadrul poliției și al serviciilor vamale. Aceste descoperiri au fost la un pas să provoace schimbarea din funcţie a ministrului justiției Benk Korthals care, însă, a reuşit să supravieţuiască dezbaterii din parlament.

---

[22] Pentru o discuție asupra acestei anchete, a se vedea website-ul Parlement & Politiek, „Parlementaire enquête opsporingsmethoden, IRT (1994-1996)" (disponibil la http://www.parlement.com/9291000/modulesf/g8pdkcx4).

Caseta 2: Elemente ale unui plan general de inspecție

- data inspecției
- baza legală pentru inspecție
- scopul inspecției
- obiectivele inspecției
- numele membrilor personalului de supraveghere care vor efectua inspecția
- desemnarea unităților din serviciu care urmează a fi inspectate
- numele persoanelor din serviciu care urmează a fi intervievate
- cerințe pentru interviuri
- lista documentelor ce urmează a fi inspectate
- cererea de documente în pregătirea inspecţiei
- resurse
- asistența administrativă
- graficul de raportare.[23]

8.4 SECURIZAREA DOCUMENTELOR ȘI A ALTOR MATERIALE

Membrii organismelor de supraveghere trebuie să fie riguroși în lucrul cu documente și note. Trebuie să se respecte regula biroului fără hârtii, iar informațiile clasificate trebuie să urmeze rutina depozitării în seifuri. Documentele clasificate, fie imprimate pe hârtie, fie arhivate digital într-un computer ori pe un dispozitiv de memorie externă, nu trebuie să părăsească biroul fără o autorizare adecvată. Înregistrările interne referitoare la surse confidențiale, martori sau alți respondenți-cheie trebuie să-și păstreze caracterul anonim. În sfârșit, toate aceste cerințe trebuie să fie prezentate explicit într-un manual intern cuprinzând procedurile corespunzătoare.

8.5 ALCĂTUIREA UNUI PLAN

Unora dintre organismele de supraveghere li se cere să pregătească un set de reglementări sau protocoale sau chiar planuri detaliate de inspecţie, care să fie aprobate înainte de începerea activităților de supraveghere. Scopul acestui exercițiu este de a evita neînțelegerile cu privire la drepturile și puterile organismului de supraveghere și cele ale serviciului de informații care este supravegheat. Printre cerințele minime specifice, incluse în astfel de documente, se

---

[23] Acest rezumat derivă dintr-un model de plan prezentat la Școala de Inspectori Generali din Armata Statelor Unite, *Intelligence Oversight Guide*, Appendix D [*Ghid pentru supravegherea serviciilor de informații* – Anexa D] (februarie 2008) (disponibil la http://www.fas.org/irp/doddir/army/ioguide.pdf).

numără identitatea unității sau misiunii supuse examinării, tehnologiile folosite și dosarele care vor fi inspectate.

Dat fiind că o supraveghere poate fi complicată, este de obicei, util ca membrii unui organism de supraveghere, chiar atunci când nu există nicio cerință în acest sens, să conceapă și să convină asupra unui scenariu comun înainte de începerea activității de supraveghere. Planurile detaliate de inspecţie, cu precădere, stimulează angajamentul celor implicaţi față de procesul de supraveghere. Mai mult, pregătirea în avans a unor proceduri amănunțite permite membrilor unui organism de supraveghere să se concentreze mai uşor asupra conținutului odată începută inspecţia.

Caseta 3: Sarcini suplimentare pentru un plan detaliat de inspecție

- Alcătuirea unui calendar pentru inspecție.
- Schițarea unei liste de respondenți.
- Redactarea unei scrisori de invitare a potențialilor respondenți și a unei scrisori către superiorii respondenților care au nevoie de autorizare pentru depunerea unei mărturii.
- Elaborarea unui protocol pentru respondenții cu statut diplomatic (privilegii și imunități).
- Stabilirea tipurilor de interviuri care vor fi realizate (confidențiale, anonime, înregistrate, etc.).
- Elaborarea protocoalelor pentru interviuri, stabilind răspunsuri la întrebări precum: Va avea respondentul acces prealabil la întrebări? I se va permite respondentului să facă uz de documente sau alte forme de suport de memorie în timpul interviului? Are respondentul dreptul de a revedea sau edita transcrierea interviului ?
- Elaborarea unui protocol pentru lucrul cu surse și informații clasificate.
- Stabilirea asistenței pentru transcriere și traducere.
- Elaborarea unui protocol pentru comunicarea publică a informaţiilor obținute din interviuri.

9. PROFESIONALISMUL ȘI CREDIBILITATEA ORGANISMELOR DE SUPRAVEGHERE

Oamenii care trăiesc în societăți democratice se așteaptă ca agențiile lor guvernamentale să respecte legile țării și, dacă nu o fac, să fie trase la răspundere de organismele de supraveghere. Datorită puterilor excepționale de care dispun serviciile de informații – care pot limita sau încălca drepturile omului – organismele care le supraveghează au, în mod corespunzător, o mare respon-

sabilitate. Așa încât, acestora din urmă le revine datoria de a demonstra, în activitatea și conduita lor publică, cele mai înalte standarde de profesionalism în supraveghere. Altminteri, credibilitatea procesului de supraveghere va avea de suferit, iar oamenii își vor pierde încrederea în instituțiile guvernamentale.

9.1 INDEPENDENȚA ORGANISMULUI DE SUPRAVEGHERE

Un organism de supraveghere nu poate fi considerat profesionist dacă independența și autonomia sa nu sunt pe deplin garantate prin lege. Totodată, profesionalismul impune ca organismele de supraveghere să fie cu desăvârșire nepartizane – adică libere față de presiunile politicilor de partid, imixtiunea executivului și presiunea exercitată de mass-media.

Practic vorbind, cea mai bună cale de a se apăra împotriva presiunii politicului sau a mass-mediei este să fie conștiente de ea. Din acest motiv, personalul organismelor de supraveghere beneficiază adesea de instruire în relaţia cu mass-media, care, printre altele, îl pregătește să răspundă la întrebări neașteptate din partea politicienilor sau a mass-mediei. Ceea ce e deosebit de important, având în vedere necesitatea de a preveni dezvăluirea accidentală de informații confidențiale atunci când se răspunde unor asemenea întrebări.

9.2 EXPERTIZA ANGAJAȚILOR DIN ORGANISMELE DE SUPRAVEGHERE

În mod ideal, membrii organismelor de supraveghere și angajații lor trebuie să aibă cunoștințe prealabile și o experiență de lucru într-o serie de agenții de securitate, inclusiv agenții de poliție și militare, precum și în servicii de informații interne și externe. Cei care nu le au trebuie să fie instruiți în cel mai scurt timp şi să fie încurajați și/sau să li se ceară să participe regulat la seminarii de pregătire și să parcurgă cu atenție regulile și regulamentele aplicabile.

9.3 INFORMAȚIILE CLASIFICATE

Una din cele mai dificile dileme profesionale cu care se confruntă personalul din organismele de supraveghere este stabilirea echilibrului optim între exigențele divergente de asigurare a transparenței și, respectiv, de secretizare (a se vedea Nathan, Instrumentul 3). Deoarece dezvăluirea anumitor informații confidențiale poate să pericliteze realmente securitatea națională, guvernele au dreptul legitim de a le păstra secrete față de publicul larg. Din acest motiv, angajații organismelor de supraveghere trebuie să obțină certificatul de securitate înainte de a lucra cu informații clasificate. Cu toate acestea, nici o secretizare prea mare nu e de dorit, în special atunci când clasificarea e folosită în exces pentru a ascunde activități stânjenitoare din punct de vedere politic (precum crearea, în SUA, a programelor secrete de detenție, interogare și extrădare). Incorecta utilizare a legilor privind secretul de stat îi poate deter-

mina pe cetățeni să își piardă încrederea în propriul guvern, subminându-se astfel legitimitatea tuturor instituțiilor guvernamentale. Mai mult, clasificarea excesivă obstrucționează o supraveghere eficace. (Această problemă e ameliorată în unele jurisdicții prin legi care autorizează puterea judecătorească să verifice dacă anumite documente au fost clasificate în mod justificat sau nu.)

10. CONDUITA ORGANISMELOR DE SUPRAVEGHERE

Maniera în care se comportă un organism de supraveghere poate avea un impact substanțial asupra eficacității sale. Dacă organismele de supraveghere nu adoptă ele însele valori precum transparența și consecvența, nu se pot aștepta, în mod legitim, ca serviciile de informații să facă acest lucru.

10.1 TRANSPARENȚA

Eficacitatea unui organism de supraveghere este susținută cel mai bine printr-o transparență maximă. Este esențial, în special, ca organismele de supraveghere să acționeze în conformitate cu standardele și protocoalele convenite, astfel încât să își poată explica întotdeauna acțiunile și să demonstreze aceeaşi responsabilitate pe care o așteaptă din partea serviciilor de informații pe care le supraveghează. Transparența unui organism de supraveghere poate fi sporită prin includerea în rapoartele sale a unor informații privind sursele consultate și termenii de referință utilizați într-o anumită investigație.

10.2 CONSECVENȚA

Șocurile sau scandalurile produc, de regulă, runde intense de supraveghere a serviciilor de informaţii, urmate de perioade de riguroasă monitorizare. Și totuși e important ca supravegherea să se petreacă fără întreruperi și nu doar ca reacție la anumite probleme. Organismele de supraveghere a serviciilor de informații pot promova o mai mare consecvență în activitatea lor prin dezvoltarea unui tipar de monitorizare și inspecție. O astfel de abordare ajută la evitarea neglijării unor aspecte sau a unor lacune în supraveghere și reduce, în ultimă instanță, posibilitatea reapariției unor eșecuri în activitatea de intelligence.[24]

[24] Loch K. Johnson, *Secret Spy Agencies and a Shock Theory of Accountability* [*Agențiile secrete de spionaj și o teorie șoc a responsabilității*], Department of International Affairs Occasional Papers (University of Georgia, School of International and Public Affairs, 2006), p. 2.

10.3 INTERACȚIUNEA CU SERVICIILE DE INFORMAȚII

Chiar dacă serviciile de informații pot părea entități birocratice închise, izolate, cele mai multe dintre ele sunt organizații care își reconsideră activitatea din dorința de a-și remedia deficiențele. Din acest motiv, organismele de supraveghere sunt interesate ca interacțiunea lor cu serviciile de informaţii să fie stimulativă, să survină la timp şi să fie instructivă. De exemplu, recomandările specifice privind acțiuni de remediere trebuie să fie prezentate sub o formă care să permită serviciilor de informații să le traducă în linii directoare concrete, în protocoale, proceduri și grafice care să aibă relevanţă în propriile lor organizații.

De asemenea, e important ca personalul de supraveghere să fie conştient de efectele adverse pe care le pot avea constatările lor asupra anumitor ofiţeri de informații şi care duc frecvent la pedepsirea acestora și, uneori, chiar la demitere. Iată de ce se recomandă, de obicei, ca membrii organismelor de supraveghere să discute asemenea chestiuni cu conducerea superioară a serviciului respectiv înainte de raportarea celor constatate.

11. RAPORTAREA

Cu toate că organismele de supraveghere a serviciilor de informaţii folosesc o gamă largă de proceduri, ele sunt obligate în toate cazurile să aducă la cunoștință rezultatele anchetelor lor. În aproape toate situațiile, legea le impune să prezinte periodic rapoarte, de regulă, anual. Asemenea rapoarte includ, în general, descrierea investigațiilor întreprinse, precum și analiza bugetară, dacă face parte din mandatul organismului de supraveghere. Rapoartele pot conține și recomandări adresate serviciilor de informații și/sau executivului pentru creşterea răspunderii, transparenţei, legalităţii şi eficacităţii serviciilor respective.

De asemenea, pe parcursul unui an, organismele de supraveghere pot elabora rapoarte speciale. Acestea pot fi tematice sau pot descrie o anumită investigație. De pildă, dacă un organism de supraveghere află despre o activitate de intelligence ce poate fi pusă sub semnul întrebării, se impune, în general, să o raporteze în timp util autorităţii competente.

Potrivit lui Aidan Wills, „De obicei, organismele de supraveghere alcătuiesc două versiuni ale rapoartelor lor. Pentru executiv și serviciile de informații elaborează o versiune ce poate conține informații clasificate; iar cea de-a doua versiune, de interes public, nu conține, în general, informații clasificate. Organismele de supraveghere se consultă cu executivul și serviciile de informații înainte de difuzarea rapoartelor publice. O asemenea consultare oferă servici-

ilor șansa de a-și face cunoscută eventuala îngrijorare față de includerea, în rapoartele respective, a unor informații sensibile.”[25]

11.1 PREZENTAREA RAPOARTELOR

Rutina prezentării de rapoarte variază de la o țară la alta. În Belgia, Comisia I trimite raportul său anual președinților celor două camere ale parlamentului și ministrului responsabil. Totuși, rapoartele speciale sunt prezentate mai întâi ministrului responsabil și abia ulterior președintelui camerei superioare a parlamentului.[26] Mai mult, rapoartele prezentate parlamentului nu conțin informații clasificate. În Canada, unde regulile de raportare sunt diferite, SIRC își prezintă raportul anual executivului, care trebuie să îl transmită parlamentului în termen de 15 zile. De asemenea, prin lege, SIRC trebuie să se consulte cu directorul CSIS înainte de a-și face public raportul.

11.2 DREPTUL DE PROPRIETATE ASUPRA RAPOARTELOR

Organismele de supraveghere trebuie să aibă control deplin asupra rapoartelor lor, inclusiv asupra conţinutului şi datei la care le prezintă. În unele cazuri, legile sau regulile de procedură pot stabili modul în care se lucrează cu informațiile clasificate sau perioada de timp după care rapoartele respective pot deveni publice. În Olanda, CTIVD acordă ministrului responsabil șase săptămâni. Dacă ministrul nu dă niciun răspuns oficial în cele șase săptămâni, raportul organismului de supraveghere este publicat.

11.3 CONSIDERENTE POLITICE

Activitatea în domeniul intelligence, care are loc la limita legitimității politice, poate fi intens controversată. Ca exemple pot fi amintite culegerea de informații în jurisdicția unei țări străine și utilizarea măsurilor speciale de investigare care încalcă drepturile omului. Prin urmare, investigațiile întreprinse în cadrul unei supravegheri atrag frecvent partizani dornici să utilizeze constatările în propriul lor avantaj politic. Cea mai bună cale de a face față unor asemenea presiuni este de a le anticipa. De exemplu, trebuie să se țină seama de calendarul politic și de efectul său asupra atenției jurnaliștilor. Anticiparea posibilelor consecințe politice ale unui raport poate ajuta la pregătirea lui. Pe de altă parte, orchestrarea excesivă a difuzării unui raport poate face ca organis-

[25] Aidan Wills, *Guidebook: Understanding Intelligence Oversight*, Toolkit – Legislating for the Security Sector [*Ghid pentru înțelegerea activității de supraveghere a serviciilor de informații*, Set de instrumente – Legiferarea pentru sectorul de securitate] (Geneva, DCAF, 2010), p. 40.

[26] Ibid., p. 37.

mul de supraveghere să pară mai curând complice decât independent și obiectiv.

11.4 IMPLEMENTAREA RAPOARTELOR

Un raport nu constituie un sfârșit în sine. Scopul lui este mai degrabă să genereze discuții asupra chestiunilor prezentate în parlament, în guvern și chiar în afara acestora. Numai astfel constatările unui raport pot duce la aplicarea recomandărilor pe care le face.

Orice raport de supraveghere, ocazional sau periodic, trebuie să menționeze clar concluziile desprinse și recomandările privind schimbările ce trebuie efectuate. Ele trebuie formulate precis și numerotate. În plus, odată ce raportul a fost prezentat autorităților competente, organismul de supraveghere trebuie să colaboreze cu acestea pentru a alcătui un calendar al aplicării. Ulterior, organismul de supraveghere trebuie să redacteze și să prezinte un raport de evaluare a implementării, prezentând măsura în care recomandările sale au fost aplicate de către respectivele servicii de informații.

11.5 ACCESIBILITATEA RAPOARTELOR

În prezent, cu ajutorul tehnologiilor moderne, precum Internet-ul, organismele de supraveghere pot face ca rapoartele lor să fie larg accesibile publicului. Ancheta din Marea Britanie referitoare la implicarea națională în războiul din Irak (ancheta Chilcot) a publicat deja pe website-ul propriu transcrierile, declarațiile martorilor și alte documente neclasificate, în pregătirea difuzării raportului său final.

Se poate întâmpla ca raportul unui organism de supraveghere să fie publicat pe un website care nu se află sub controlul său – așa cum e un website ministerial sau parlamentar. Ca să se asigure că rapoartele pe care le elaborează rămân accesibile publicului, organismul respectiv trebuie să insiste să i se aducă la cunoștință anticipat ori de câte ori se decide eliminarea rapoartelor sale de pe website-ul în cauză. În consecință, e recomandabil ca organismele de supraveghere să aibă în permanență website-uri publice pentru a facilita accesul la rapoarte și la alte documente.

12. CONSTATĂRI POSIBILE

Organismele de supraveghere a serviciilor de informații analizează o gamă largă de chestiuni, dintre care unele sunt generale (precum cadrul legislativ aplicabil unui serviciu) și altele – specifice (așa cum e investigarea unui anumit incident). În continuare se regăsesc exemplele a trei constatări posibile, rezul-

tate din investigațiile de supraveghere. Fiecare din ele prezintă recomandări de ameliorare, ce ar putea rezulta în urma investigațiilor.

12.1 UN SERVICIU DE INFORMAȚII A EȘUAT ÎN VERIFICAREA INFORMAȚIILOR FURNIZATE DE PARTENERI STRĂINI

Se poate întâmpla ca serviciile de informații, în special atunci când acționează în cooperare cu parteneri străini, să nu verifice în mod corespunzător informațiile pe care le primesc din partea unor surse din afară. În 2009, în Olanda, de pildă, CTIVD a investigat utilizarea de către Serviciul General de Informații și Securitate (GISS) a informațiilor provenite din străinătate și a constatat că GISS nu a reușit, în repetate rânduri, să stabilească, așa cum impunea legea, dacă un serviciu străin de informații se califica pentru o relație de cooperare. Potrivit raportului final al CTIVD, „Nu a fost identificat niciun proces structurat de luare a deciziilor." În schimb, continua raportul, „deciziile erau luate frecvent într-o manieră *ad hoc*," pe care CTIVD a criticat-o ca fiind „prea limitată" și „de nedorit." În consecință, GISS a fost sfătuit să facă evaluări atente nu numai atunci când inițiază o nouă relație de cooperare, ci și în privința relațiilor deja stabilite.[27]

Realizarea unor asemenea evaluări înainte de a acționa pe baza informațiilor primite sunt deosebit de importante atunci când acele informații ar fi putut fi obținute prin tortură. Din acest motiv, Comisia de anchetă privind acțiunile oficialilor canadieni în cazul Maher Arar a recomandat ca toate acordurile de cooperare cu străinătatea să fie prezentate spre examinare, ca regulă generală, organismelor de supraveghere.[28] Într-un mod similar, Raportorul special al ONU a recomandat ca țările să includă în acordurile lor de schimb de informații o clauză conform căreia aplicarea acestor acorduri să fie supusă examinării de către organismele lor respective de verificare și care să afirme că acele organisme de verificare au competența de a coopera între ele în vederea

[27] Bert van Delden, „Partners in Business?" [„Parteneri în afaceri?"] (expunere la cea de-a 6-a Conferință a comisiilor parlamentare pentru supravegherea serviciilor de informații și securitate din statele membre ale Uniunii Europene, Bruxelles, 30 septembrie – 1 octombrie 2010), p. 4 (disponibil la http://www.parlement-eu2010.be/pdf/30sep-1okt-Thema3-Bert%20Van%20Delden.pdf).

[28] Comisia de anchetă privind acțiunile oficialilor canadieni în cazul Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* [*Un nou mecanism de verificare a activităților RCMP legate de securitatea națională*] (2006) (disponibil la http://www.sirc-csars.gc.ca/pdfs/cm_arar_rcmpgrc-eng.pdf).

evaluării performanțelor uneia sau ambelor părți.[29] (Pentru alte detalii privind schimbul de informații, a se vedea Roach – Instrumentul 7).

12.2 UN SERVICIU DE INFORMAȚII ȘI-A DEPĂȘIT MANDATUL

Organismele de supraveghere trebuie să analizeze cu regularitate dacă activitățile unui serviciu de informații depășesc mandatul pe care îl are, cu deosebire în privința utilizării puterilor speciale pentru culegerea de informații (a se vedea Hutton – Instrumentul 5). Dacă serviciul în cauză nu a respectat, în mod real, limitele autorității sale, organismul de supraveghere trebuie să îl tragă la răspundere. Ceea ce se poate realiza prin raportarea încălcării limitelor către autoritățile competente și, dacă mandatul organismului de supraveghere o permite, prin anularea uneia sau mai multor puteri speciale ale serviciului respectiv.

După ce a stabilit, printre altele, că RCMP și-a depășit mandatul, Comisia Arar a recomandat ca RCMP să respecte, din acel moment, rolul distinct pe care îl are CSIS în cadrul comunității de informații din Canada.[30]

12.3 DOMENIUL INTELLIGENCE A FOST POLITIZAT

Informațiile pot fi politizate pe mai multe căi, dintre care nu toate implică serviciul de informații care le produce. Cu toate astea, politizarea rezultă cel mai frecvent dintr-o relație prea strânsă între executiv și oficialii serviciului, care, conștient sau inconștient, adaptează informațiile în așa fel, încât să sprijine pozițiile recunoscute ale executivului („informații care plac"). O formă înrudită de politizare se referă la folosirea serviciilor de informații de către oficialii guvernamentali pentru a obține informații ce aduc prejudicii oponenților lor politici. Politizarea poate rezulta și în cadrul unui serviciu de informații, din rivalitatea între analiști, care intră în competiție pentru a produce informații în măsură să determine acțiuni în justiție, cu scopul de a avansa în carieră.

---

[29] Consiliul Națiunilor Unite pentru Drepturile Omului, *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development: Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*. Cu referire la C. Forcese, „The Collateral Casualties of Collaboration: the Consequence for Civil and Human Rights of Transnational Intelligence Sharing" [„Victimele colaterale ale colaborării: consecințele schimbului transnațional de informații asupra drepturilor civile și a drepturilor omului"] (contribuție scrisă la seminarul DCAF privind responsabilitatea în cooperarea internațională din domeniul intelligence, Oslo, 17 octombrie 2008).

[30] Comisia de anchetă privind acțiunile oficialilor canadieni în cazul Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities*.

Un organism de supraveghere care descoperă probe privind politizarea muncii de informații trebuie să recomande parlamentului să dezbată în mod deschis obiectivele de politică externă și de apărare stabilite. Totodată, el trebuie să analizeze care sunt măsurile de siguranță ce ar putea fi luate pentru a preveni utilizarea pe viitor a informațiilor drept instrument politic.[31]

13.RECOMANDĂRI

- Mandatul unui organism de supraveghere a serviciilor de informații trebuie să fie formulat în mod precis şi în detaliu, de preferat ca parte a unui cadru legislativ cuprinzător, care înglobează supravegherea tuturor serviciilor de informații.
- Dacă mandatul unui serviciu de informații este modificat, trebuie revizuit în mod corespunzător și mandatul organismului de supraveghere aferent.
- Mandatele organismelor naționale de supraveghere a serviciilor de informații, luate în ansamblu, trebuie să acopere întreaga comunitate de informații dintr-o țară, inclusiv serviciile civile și militare, precum și departamentele și oficialii care le acordă sprijin.
- Competențele care fac parte din mandatul unui organism de supraveghere, referitoare la acces, investigare, inspecție și aprobare, trebuie să fie pe măsura competențelor de care dispun serviciile de informații supravegheate de respectivul organism.
- Un organism de supraveghere a serviciilor de informații trebuie să aibă autoritatea de a face inspecții pe teren, de a organiza audieri cu ușile deschise și închise, precum și de a avea acces la informațiile clasificate din documente, baze de date și alte fișiere computerizate.
- Un organism de supraveghere a serviciilor de informații trebuie să poată efectua supravegherea *ex post*. În cazul excepțional în care un organism efectuează o supraveghere *ex ante*, membrii acestuia trebuie să fie verificați de o agenție de securitate pentru a asigura protecția identității surselor și a altor informații operaționale.

[31] Pentru o discuție ulterioară, a se vedea Monica den Boer, „Keeping 'Spies & Spooks' on the Right Track: Ethics in the Post 9/11 Intelligence Era" [„Menținerea spionilor britanici și americani pe drumul cel bun: etica în era informațiilor după 11/9"], în *Ethics and Security*, editori Monica den Boer și Emile Kolthoff (Haga: Eleven, 2010), pp. 57–83.

- Pentru a-și organiza activitatea și a stimula angajamentul părților implicate, un organism de supraveghere a serviciilor de informații trebuie să elaboreze întotdeauna un plan de supraveghere.
- Un organism de supraveghere a serviciilor de informații trebuie să mențină un înalt nivel de profesionalism. Astfel, se va consolida nu numai legitimitatea organismului de supraveghere, dar, indirect, și cea a serviciilor de informații pe care le supraveghează.
- Conduita unui organism de supraveghere a serviciilor de informații trebuie să fie transparentă, consecventă și responsabilă.
- Un organism de supraveghere a serviciilor de informații trebuie să publice periodic (anual) rapoarte în care să-și prezinte activitățile și constatările. De asemenea, el trebuie să publice, dacă este cazul, rapoarte ocazionale în care să prezinte anumite investigații.
- Rapoartele unui organism de supraveghere a serviciilor de informații trebuie să fie larg accesibile publicului.
- Un organism de supraveghere a serviciilor de informații trebuie să prezinte conducerii superioare a serviciilor respective o primă versiune a constatărilor sale în vederea obținerii unei reacții din partea lor în termenul legal stabilit prin mandat.
- Rapoartele unui organism de supraveghere a serviciilor de informații trebuie să includă întotdeauna recomandări care pot fi aplicate de serviciile în cauză.
- Un organism de supraveghere a serviciilor de informații trebuie să monitorizeze activ punerea în practică a recomandărilor sale și să publice rapoarte de evaluare a implementării.

INSTRUMENTUL 5

Supravegherea culegerii de informații

Lauren Hutton



5

Supravegherea culegerii de informații

Lauren Hutton

1. INTRODUCERE

Scopul acestui instrument este de a examina rolul pe care îl joacă organismele de supraveghere în monitorizarea funcțiilor de culegere a informațiilor de către serviciile de informații. Produsul de intelligence este rezultatul unui proces cu mai multe etape, care presupune trasarea sarcinilor, planificarea, culegerea de informații, analizarea și diseminarea lor. Însă, din toate aceste etape, culegerea de informații, în special prin mijloace secrete, rămâne trăsătura definitorie a serviciilor de informații, cel puțin în accepțiunea publică. Culegerea de informații este unul din cele mai controversate aspecte ale activității în domeniul intelligence și prezintă o serie de provocări ieșite din comun pentru organismele de supraveghere, care au datoria de a susține idealurile democratice.

Prima parte a prezentului instrument va analiza câteva dintre metodele prin care serviciile de informații obțin informații. După care, vor fi studiate modalitățile prin care țările democratice pot utiliza legislația, autorizarea și supravegherea pentru a se asigura că drepturile omului sunt respectate ori de câte ori se folosesc metode secrete.

2. SURSELE ȘI METODELE DE CULEGERE A INFORMAȚIILOR

Produsul de intelligence se bazează pe informații culese din diferite surse. Dat fiind că nicio sursă unică nu e în măsură să ofere îndeajuns de multe informații pentru deplina înțelegere a unei anumite probleme, serviciile de informații folosesc surse multiple pentru a ajunge la cea mai precisă imagine a evenimentelor. Aceste surse sunt împărțite pe categorii, în funcție de tipul lor:

- informații din surse umane (HUMINT), așa cum sunt informatorii;
- informații din semnale (SIGINT), așa cum sunt interceptările unor comunicații;

- informații din surse deschise (OSINT), așa cum sunt relatările mass-mediei;
- informații din imagini (IMINT), așa cum sunt fotografiile din satelit.

Metodele de culegere a informațiilor pot fi la vedere sau sub acoperire. Metodele la vedere sunt cel mai adesea folosite pentru a strânge OSINT, deoarece informațiile sunt deținute în mod deschis și sunt disponibile public. În cazul metodelor sub acoperire sau clandestine, culegerea informațiilor despre ținte se face în secret, fără știința acestora. Metodele sub acoperire pot include folosirea informatorilor, urmărirea electronică, interceptarea comunicațiilor, urmărirea fizică și imagini culese de la distanță. Atunci când asemenea metode sunt folosite într-un mod care încalcă dreptul unei persoane la viață privată, ele sunt denumite „metode intruzive de investigare." Iar tehnicile aferente sunt numite „măsuri speciale de investigare" sau „tehnici speciale de investigare."

Consiliul Europei a definit *tehnicile speciale de investigare* drept „tehnici aplicate de autoritățile competente în contextul cercetărilor penale, având ca scop depistarea și investigarea unor infracțiuni grave și a suspecților, și care urmăresc culegerea de informații în așa fel, încât persoanele țintă să nu intre în alertă."[1] În acest context, *autorități competente* pot fi ori serviciile de informații, ori agențiile de aplicare a legii. E important să se observe că, în multe țări, serviciile de informații folosesc astfel de măsuri nu numai în cadrul cercetărilor penale, dar și în investigațiile preventive, legate de securitatea națională. Ca principiu general, metoda utilizată pentru culegerea de informații trebuie să se bazeze pe tipul de informație necesar, pe scopul efortului de culegere și pe contextul operațional, legal și politic în care acționează serviciile de informații.

3. IMPACTUL CULEGERII DE INFORMAȚII ASUPRA DREPTURILOR OMULUI

Serviciile de informații culeg informații pentru a-i ajuta pe oficialii guvernamentali să elaboreze politici și să ia decizii strategice și operaționale. Modul în care obțin informațiile trebuie să fie compatibil cu prioritățile și valorile

---

[1] Consiliul Europei, Comitetul Miniștrilor, *Recommendation Rec(2005)10 of the Commitee of Ministers to member states on „special investigative techniques" in relation to serious crimes including acts of terrorism* [*Recomandarea Rec(2005)10 a Comitetului Miniștrilor către statele membre cu privire la «tehnicile speciale de investigare» în legătură cu crimele grave, inclusiv actele de terorism*] (20 aprilie 2005), Rec(2005)10, Capitolul I (disponibil la https://wcd.coe.int/ViewDoc.jsp?id=849269&Site=CM).

societății pe care o servesc.[2] În țările democratice, serviciile de informații trebuie să respecte drepturile omului, statul de drept și principiile guvernanței democratice, inclusiv responsabilitatea, transparența și participarea la luarea deciziilor. Munca de informații trebuie să se desfășoare între acești parametri, de la atribuirea sarcinilor până la diseminarea informațiilor.

Strângerea de informații despre amenințările la adresa securității poate avea un impact direct asupra drepturilor fundamentale ale indivizilor.[3] În conformitate cu raportul din 2008 al Comisiei ministeriale de verificare a serviciilor de informaţii din Africa de Sud, care investiga presupuse abuzuri de putere săvârșite de Agenția Națională de Informații, „metodele intruzive de investigare pot avea un rol crucial în aducerea la lumină a activităților și conspirațiilor criminale, însă ele pot fi folosite și în mod incorect pentru a submina procesul democratic, a interveni în activitatea politică și socială legală și pentru a avantaja, în mod incorect, anumiți politicieni și partide."[4]

Cu toate că utilizarea de către stat a metodelor intruzive este întotdeauna sensibilă din punct de vedere constituțional și politic, folosirea lor de către serviciile de informații trebuie tratată cu deosebită prudență. Motivele pentru o asemenea prudență, enumerate de raportul Comisiei ministeriale de verificare,[5] includ următoarele:

- Ținta unei investigații poate să nu afle niciodată despre utilizarea metodelor intruzive și, în consecință, nu va fi capabilă să obiecteze în privința lor și nici să le conteste validitatea în instanță.

---

[2] Pentru o dezbatere mai amplă asupra acestui punct, a se vedea Ronnie Kasrils, „To spy or not to spy? Intelligence and democracy in South Africa" [„A spiona sau a nu spiona? Intelligence și democrație în Africa de Sud"], în *To spy or not to spy? Intelligence and democracy in South Africa*, ed. Lauren Hutton (Pretoria: Institute for Security Studies, 2009), pp. 9–22.

[3] Pentru o dezbatere mai amplă asupra acestui punct, a se vedea Marina Caparini, „Controlling and Overseeing Intelligence Services in Democratic States" [Controlul și supravegherea serviciilor de informații în statele democratice"], în *Democratic Control of Intelligence Services: Containing Rogue Elephants*, editori: Hans Born și Marina Caparini (Aldershot, UK: Ashgate, 2007), p. 3–24.

[4] Africa de Sud, Comisia ministerială de verificare a serviciilor de informaţii, Intelligence in a Constitutional Democracy: *Final Report to the Minister for Intelligence Services*, *the Honourable Mr. Ronnie Kasrils*, *MP* [Intelligence într-o democrație constituțională: *Raport final în atenția ministrului pentru serviciile de informații, Hon. Mr. Ronnie Kasrils, MP*] (10 septembrie 2008) (disponibil la http://www.ssronline.org/document_result.cfm?id=3852).

[5] Ibid., pp. 158–159.

- Înaltul nivel de secretizare ce însoțește metodele intruzive reduce capacitatea organismelor de supraveghere de a monitoriza utilizarea lor și de a detecta posibile abuzuri și ilegalități.
- Măsura în care metodele intruzive încalcă dreptul individului la viață privată poate fi mult mai mare decât este necesar sau se intenționează.
- Pe lângă încălcarea vieții private a țintei, metodele intruzive afectează adesea drepturile la viață privată ale unor indivizi cu care ținta intră în contact, chiar dacă acești indivizi nu sunt supuși investigației.
- Informațiile sensibile referitoare la țintă și la persoanele cu care aceasta intră în contact sunt înregistrate și păstrate de serviciile de informații pe o perioadă de timp mai mare decât cea a investigației și, uneori, sunt folosite pentru alte scopuri.

Uneori, se face o distincție între utilizarea în străinătate și utilizarea pe plan intern a tehnologiei de interceptare, deoarece, pe plan intern, există pericolul ca executivul să folosească sisteme clandestine de interceptare în scopuri partizane, spre exemplu, pentru spionarea oponenților politici. Pe de altă parte, interceptarea comunicațiilor în străinătate nu periclitează în general ordinea democratică internă.

În țările democratice, organismele de supraveghere a serviciilor de informații au dreptul legitim și, deseori, responsabilitatea legală de a se asigura că serviciile au o conduită compatibilă cu ordinea constituțională. Responsabilitatea organismelor de supraveghere se extinde de obicei asupra întregului proces de intelligence, însă zona culegerii de informații necesită o atenție specială, date fiind pericolele la care sunt expuse valorile democratice prin folosirea metodelor sub acoperire, intruzive. Mai precis, organismele de supraveghere trebuie să monitorizeze îndeaproape utilizarea tuturor metodelor de acest tip pentru a se asigura că serviciul respectiv de informații își menține conduita în limitele legii.

3.1 PROTEJAREA DREPTULUI LA VIAȚĂ PRIVATĂ

Dreptul restricționat sau încălcat cel mai frecvent de serviciile de informații este dreptul la viață privată. În consecință, o funcție cheie a organismelor de supraveghere trebuie să fie aceea de a se asigura că serviciile culeg informații într-un mod care respectă legislația națională și internațională în privința dreptului la viață privată.

Raportorul special al Națiunilor Unite pentru promovarea și protejarea drepturilor omului și libertăților fundamentale în contextul combaterii terorismului a

definit dreptul la viață privată ca „presupunerea că indivizii trebuie să aibă un spațiu de dezvoltare, interacțiune și libertate autonome, o ‚sferă privată', cu sau fără interacțiune cu ceilalți, ferită de intervenția statului și de intervenția excesivă, nesolicitată a altor indivizi."[6]

În mod asemănător, Articolul 17 al *Convenției internaționale cu privire la drepturile civile și politice* afirmă că:

> 1. Nimeni nu va putea fi supus vreunor imixtiuni arbitrare sau ilegale în viața particulară, în familia, domiciliul sau corespondența sa, nici la atingeri ilegale aduse onoarei și reputației sale.
> 2. Orice persoană are drept la protecția legii împotriva unor asemenea imixtiuni sau atingeri.

Având 167 de semnatari, *Convenția internațională cu privire la drepturile civile și politice* reprezintă baza dreptului internațional referitor la viața privată. Deoarece, potrivit acesteia, viața privată este un drept fundamental al omului, acțiunile unui guvern care limitează acest drept trebuie să fie autorizate prin legislația națională pentru un scop anume, legitim.

După cum a stabilit Curtea Europeană a Drepturilor Omului, protejarea securității naționale este un scop legitim pentru limitarea unui drept al omului, așa cum este dreptul la viață privată. Cu toate acestea, potrivit Curții, orice astfel de limitare trebuie impusă în conformitate cu legislația națională, care trebuie să includă măsuri de siguranță împotriva abuzului și căi de atac, dacă totuși au loc abuzuri.[7]

Utilizarea de către un serviciu de informații a metodelor intruzive, sub acoperire, de culegere de informații constituie o limitare a dreptului la viață privată. În consecință, e necesar ca utilizarea lor să fie autorizată de legislația națională și să se recurgă la ele numai pentru scopuri bine precizate, legitime. În Africa

---

6 Consiliul Națiunilor Unite pentru Drepturile Omului, *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development: Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, [*Promovarea și protejarea tuturor drepturilor omului, a drepturilor civile, politice, economice, sociale și culturale, inclusiv dreptul la dezvoltare: Raportul Raportorului special pentru promovarea și protejarea drepturilor omului și libertăților fundamentale în contextul combaterii terorismului*], Document al Națiunilor Unite A/HRC/10/3 (4 februarie 2009), p. 6–7 (disponibil la www.unhcr.org/refworld/pdfid/49b138c32.pdf).

7 Consiliul Europei, Comisia Europeană pentru Democrație prin Drept (Comisia de la Veneția), *Report on the democratic oversight of the security services* [*Raport privind controlul democratic al serviciilor de securitate*], CDL-AD(2007)016 (2007) (disponibil la http://www.venice.coe.int/docs/2007/CDL-AD%282007%29016-e.asp).

de Sud, fostul inspector general pentru informații a interpretat acest principiu în felul următor:

> O limitare a drepturilor poate fi justificată în temeiul unor amenințări la adresa securității naționale. Asemenea limitare trebuie să facă față testului de proporționalitate, care pune în balanță natura dreptului și importanța scopului pentru care se dorește limitarea. Ca atare, competența de a strânge informații trebuie să fie dublată de măsuri de siguranță la fel de puternice, care să apere drepturile constituționale ale cetățenilor și să susțină o societate deschisă și democratică.[8]

3.2 IMPACTUL TEHNOLOGIEI ASUPRA CULEGERII DE INFORMAȚII

Tehnologia modernă a informației și comunicațiilor face posibil ca persoane din întreaga lume să comunice instantaneu și permite informațiilor să străbată distanțe imense într-o clipă. Totodată însă, ea oferă guvernelor posibilitatea să desfășoare o activitate de urmărire la un nivel fără precedent. Folosind dispozitive tehnologice avansate, serviciile de informații pot să culeagă informații în masă, obținând mult mai multă informație decât pot absorbi și analiza. Deoarece, prin natura sa, culegerea de informații de acest tip nu face diferențieri, ea poate încălca drepturi ale omului și ar trebui să fie realizată doar într-un cadru legal, care protejează dreptul la viață privată.

Sistemul de interceptare ECHELON oferă un exemplu util. Acest sistem – operat în comun de SUA, Marea Britanie, Australia, Canada și Noua Zeelandă, ca parte a unui aranjament colectiv de securitate – interceptează semnalele transmise spre și dinspre sateliți orbitali. În anul 2000, Parlamentul European a creat o comisie temporară care să investigheze impactul potențial al sistemului ECHELON asupra drepturilor omului, din perspectiva legislației Uniunii Europene (UE). Raportul final al comisiei a ajuns la concluzia că sistemele de interceptare în masă, precum ECHELON, sunt susceptibile să încalce dreptul la viață privată, deoarece nu se conformează principiului proporționalității în privința utilizării metodelor intruzive. Recunoscând faptul că asemenea sisteme de interceptare pot fi justificate din rațiuni de securitate națională, comisia a recomandat ca utilizarea lor să fie reglementată de o legislație clară și accesibilă și ca statele membre UE să stabilească o supraveghere riguroasă.[9]

---

8 Africa de Sud, Comisia ministerială de verificare a serviciilor de informaţii, Intelligence in a Constitutional Democracy: *Final Report to the Minister for Intelligence Services, the Honourable Mr. Ronnie Kasrils, MP*.

9 Parlamentul European, Comisia temporară privind sistemul de interceptare ECHELON, *Draft document on the existence of a global system for intercepting private and commercial communications (ECHELON interception system)* [*Proiect de*

4. CADRUL LEGAL PENTRU CULEGEREA DE INFORMAȚII

În cele mai multe țări democratice, culegerea informațiilor de către serviciile de informații este guvernată de un cadru legal care asigură responsabilitatea și transparența. De regulă, aceasta se face mutând responsabilitățile de autorizare și supraveghere din sfera exclusivă a executivului și distribuindu-le (în diverse proporții) între parlament, puterea judecătorească și alte entități ce nu fac parte din puterea executivă.

Dreptul internațional poate servi drept bază pentru dezvoltarea legislației naționale. De exemplu, în 2005, Consiliul Europei a emis următoarele recomandări în vederea elaborării legislației naționale referitoare la utilizarea tehnicilor speciale de investigare în cazul cercetărilor penale: [10]

1. Statele membre, în conformitate cu cerințele Convenției europene a drepturilor omului (ETS No. 5), trebuie să definească în legislația lor națională circumstanțele și condițiile în care autoritățile competente sunt împuternicite să recurgă la utilizarea tehnicilor speciale de investigare.
2. Statele membre, potrivit paragrafului 1, trebuie să ia măsurile legislative corespunzătoare, prin care să permită utilizarea tehnicilor speciale de investigare în vederea punerii lor la dispoziția autorităților competente respective, în măsura în care acest lucru este necesar într-o societate democratică și este considerat a fi adecvat pentru realizarea de o manieră eficientă a cercetărilor și urmăririlor penale.
3. Statele membre trebuie să ia măsurile legislative corespunzătoare pentru a asigura un control adecvat al aplicării tehnicilor speciale de investigare de către autoritățile judiciare sau alte organisme independente, prin intermediul autorizării prealabile, al supravegherii pe perioada anchetei sau al verificării ex post facto.

În general, legislația națională privind utilizarea metodelor intruzive, sub acoperire, de culegere a informațiilor trebuie să specifice:

- când pot fi utilizate asemenea metode;
- care e pragul necesar de suspiciune ce trebuie atins;

---

document referitor la existența unui sistem global pentru interceptarea comunicațiilor private și comerciale (Sistemul de interceptare ECHELON)] (2001) (disponibil la http://cryptome.org/echelon-ep.htm).

[10] Consiliul Europei, Comitetul Miniștrilor, *Recommendation Rec(2005)10 of the Commitee of Ministers to member states on "special investigative techniques" in relation to serious crimes including acts of terrorism* [*Recomandarea Rec(2005)10 a Comitetului Miniștrilor către statele membre cu privire la «tehnicile speciale de investigare» în legătură cu crimele grave, inclusiv actele de terorism*] (20 aprilie 2005), Rec(2005)10, Capitolul II (a) (disponibil la https://wcd.coe.int/ViewDoc.jsp?id=849269&Site=CM).

- ce restricții și ce limitări se aplică;
- ce autorizări sunt necesare.

Exemple de legislație națională specifică ce reglementează utilizarea pe plan intern a metodelor sub acoperire, intruzive, de culegere a informațiilor includ „Legea telecomunicațiilor (interceptare și acces)” din Australia; „Legea privind asistența în materie de comunicații în scopul aplicării legii” din Australia; „Legea privind supravegherea informațiilor externe” din SUA și „Legea de reglementare a puterilor de investigare” din Marea Britanie. Orice lege de acest gen trebuie să abordeze trei chestiuni principale:

- obiectivele admisibile;
- proporționalitatea;
- autorizarea și supravegherea.

Mai general spus, aceste legi trebuie să impună autorităților competente să fie îndeajuns de sigure că metodele sub acoperire, intruzive vor conduce la obținerea informațiilor căutate.

4.1 OBIECTIVELE ADMISIBILE

Obiectivele admisibile pentru utilizarea metodelor sub acoperire, intruzive, de culegere a informațiilor diferă semnificativ de la un stat la altul. În unele țări, după cum a recomandat Consiliul Europei, efectuarea unei cercetări penale este un obiectiv admisibil.[11] În alte state, protejarea securității naționale și apărarea ordinii democratice sunt și ele obiective admisibile. Secțiunea 3(1) din „Legea privind restricționarea caracterului privat al corespondenței, poștei și telecomunicațiilor” din Germania împuternicește guvernul german (adică serviciile de securitate, incluzând poliția și serviciile de informații) să ordone restricționări ale dreptului unui individ la viață privată dacă „indicii concrete generează suspiciunea că o persoană plănuiește, comite sau a comis” o crimă împotriva:

- păcii;
- ordinii democratice;
- securității naționale;
- trupelor de securitate staționate în Germania.

Termenul de *indicii concrete* stabilește un nivel foarte înalt al pragului care trebuie atins înainte de a putea utiliza metode sub acoperire, intruzive. Pentru a se asigura faptul că există motive însemnate pentru utilizarea metodelor in-

[11] Ibid., Capitolul II (b) (4).

truzive de investigare, o atare justificare trebuie inclusă în cererea de autorizare.

4.2 PROPORȚIONALITATEA

Legislația care reglementează utilizarea metodelor sub acoperire, intruzive, de culegere a informațiilor trebuie să impună ca gradul de intruziune să fie proporțional cu scopul investigației. În această privință, Consiliul Europei a recomandat ca tehnicile speciale de investigare să fie utilizate doar atunci când:

- există motive verosimile pentru a crede că o infracțiune serioasă a fost comisă ori este în curs de planificare;
- a fost analizată corespunzător „proporționalitatea între efectele produse de utilizarea tehnicilor speciale de investigare și scopul care a fost identificat.”[12]

Consiliul a recomandat în continuare ca statele membre să utilizeze metode mai puțin intruzive ori de câte ori „asemenea metode permit ca delictul respectiv să fie depistat, prevenit sau urmărit cu eficacitate corespunzătoare.”[13] Linii directoare de acest gen permit utilizarea metodelor intruzive în scopuri legitime, menținând, în același timp, la minimum abuzul și încălcarea drepturilor omului.

Principiul proporționalității e mai dificil de aplicat în raport cu amenințările la adresa securității naționale. Principalul scop trebuie să fie asigurarea faptului că informațiile culese cu ajutorul metodelor intruzive nu puteau fi obținute prin alte metode mai puțin intruzive și că, prin utilizarea metodelor intruzive, se pot obține informațiile căutate. De pildă, în Germania, un ordin de utilizare a metodelor de culegere care limitează dreptul la viață privată poate fi emis numai „în situația în care folosirea unei alte metode de investigare a faptelor ar fi inutilă sau ar face ca investigația să fie considerabil mai dificilă.”[14]

4.3 AUTORIZAREA ȘI SUPRAVEGHEREA

Pentru a preveni utilizarea abuzivă a metodelor sub acoperire, intruzive, de culegere de informații, cadrul legal trebuie să cuprindă atât procedurile de autorizare (ce revin conducerii superioare a serviciilor de informații și puterii ju-

---

[12] Ibid., Capitolul II (b) (5).

[13] Ibid., Capitolul II (b) (6).

[14] Germania, Act Restricting the Privacy of Correspondence, Posts and Telecommunications [Lege privind restricționarea caracterului privat al corespondenței, poștei și telecomunicațiilor] (26 iunie 2001), în *Federal Law Gazette I*, p. 1254, revizuită 2298, ultima dată amendată de Articolul 1 al Legii din 31 iulie 2009, *Federal Law Gazette I*, p. 2499, Secțiunea 3 (2).

diciare), cât și mecanismele de supraveghere (care implică parlamentul și organismele specializate de supraveghere). Structurile adecvate de autorizare și supraveghere vor fi prezentate în detaliu în următoarele două secțiuni. Aceste niveluri de autorizare și supraveghere nu se exclud reciproc, iar un sistem cuprinzător și robust pentru asigurarea răspunderii și transparenței ar putea îngloba mai multe niveluri de autorizare și mai multe mecanisme de supraveghere.

5. AUTORIZAREA OPERAȚIUNILOR DE CULEGERE A INFORMAȚIILOR

Diferitele tipuri de culegere a informațiilor necesită diferite grade de autorizare. De pildă, urmărirea fizică, deși sub acoperire, nu este puternic intruzivă; așadar, o autorizare internă în cadrul serviciului de informații este, de obicei, suficientă. Însă, ascultarea unui telefon sau interceptarea corespondenței reprezintă o încălcare mai gravă în raport cu niște așteptări rezonabile în ceea ce privește viața privată și, de aceea, au nevoie de o autorizare de la un nivel mai înalt, așa cum ar fi din partea ministrului responsabil pentru activitatea de intelligence și/sau din partea unui judecător. Orice reluare a operațiunilor de culegere de informații trebuie să implice același nivel de autorizare ca în solicitarea inițială.

5.1 AUTORIZAREA INTERNĂ

Cerința privind autorizarea de către conducerea superioară a unui serviciu de informații a folosirii tehnicilor speciale de investigare stabilește responsabilitățile în cadrul serviciului și constituie un obstacol major în calea unei conduite incorecte. Cu toate că această cerință poate să nu fie suficientă *per se* pentru a preveni abuzurile, ea denotă că opțiunea de a limita dreptul unui individ la viața privată reprezintă o decizie serioasă, care cântărește greu și care nu poate fi luată cu ușurință. În cadrul serviciului, autoritatea decidentă trebuie să fie structurată astfel, încât, dacă gradul de invadare a vieții private va fi mai mare, va crește corespunzător și nivelul care trebuie să acorde autorizarea necesară.

5.2 AUTORIZAREA DE CĂTRE EXECUTIV

Serviciile de informații sunt controlate de executiv, care le stabilește prioritățile și le dirijează activitățile. În mod normal, aceasta este responsabilitatea ministrului desemnat. Același ministru poate fi responsabil și pentru autorizarea anumitor operațiuni de culegere de informații. Așa cum cerințele de autorizare internă atrag răspunderea conducerii superioare a serviciului pentru utilizarea tehnicilor speciale de investigare, tot așa, procedurile de autorizare la

nivelul executivului atrag răspunderea ministrului cu atribuții în domeniu pentru decizia de a aproba anumite măsuri.

Abuzurile la nivel ministerial înseamnă, cel mai adesea, utilizarea aparatului de culegere a informațiilor de care dispune un serviciu pentru a obține informații confidențiale despre oponenții politici ai guvernului. Din acest motiv, în cazul utilizării pe plan intern a metodelor sub acoperire de culegere de informații, cadrul legal trebuie să prevadă proceduri de autorizare care:

- stabilesc limite pentru ceea ce miniștrii pot cere serviciilor să facă.
- impun autorizarea judiciară, pe lângă aceea ministerială, pentru folosirea metodelor intruzive de culegere a informațiilor.
- creează un mecanism prin care ofițerii de informații pot raporta conduita incorectă.
- înființează sau desemnează un organism independent de supraveghere pentru a verifica modul de desfășurare a unor asemenea operațiuni.

5.3 AUTORIZAREA JUDICIARĂ

În cele mai multe țări democratice, o responsabilitate tradițională a puterii judiciare este de a proteja drepturile omului ale indivizilor. În virtutea acestui rol, este firesc ca judecătorii să aibă sarcina de a pune în balanță protejarea drepturilor omului în raport cu necesitățile serviciilor de informații în materie de culegere de informații. În consecință, este o practică obișnuită ca legislația națională să impună serviciilor de informații să obțină autorizarea judiciară (de obicei, sub forma unui mandat) înainte de a încălca dreptul unei persoane la viața privată. Deoarece sunt produsul unei evaluări imparțiale, asemenea mandate sunt considerate a fi un mijloc important de reducere a potențialelor abuzuri.[15] În plus, după cum se remarcă în raportul Comisiei de la Veneția privind controlul democratic al serviciilor de securitate, cerințele referitoare la autorizarea judiciară fac ca preocuparea pentru securitate să se subordoneze legii și, prin aceasta, instituționalizează respectul față de lege.[16]

---

[15] Pentru o discuție mai amplă asupra acestui punct, a se vedea Gregory Rose and Diana Nestorovska, „Terrorism and National Security Intelligence Laws: Assessing Australian Reforms” [„Terorismul și legile privind informațiile de securitate națională: evaluarea reformelor australiene”], în *LAWASIA Journal* (2005), pp. 127–155.

[16] Consiliul Europei, Comisia Europeană pentru Democrație prin Drept (Comisia de la Veneția), *Report on the democratic oversight of the security services* [*Raport privind controlul democratic al serviciilor de securitate*], CDL-AD(2007)016 (2007), pp. 44–45 (disponibil la http://www.venice.coe.int/docs/2007/CDL-AD%282007%29016-e.asp).

Caseta 1: Cerințele pentru solicitarea unei autorizări judiciare în Canada

„Legea privind Serviciul Canadian pentru Informații de Securitate” impune ca cererile serviciilor de informații în vederea obținerii mandatelor judiciare de interceptare a comunicațiilor să cuprindă următoarele: [17]

- faptele în temeiul cărora poate fi justificată convingerea că există o amenințare la adresa securității naționale;
- dovada că au fost încercate tehnici mai puțin intruzive care au eșuat sau motivele pentru care acestea nu au șanse de reușită;
- tipul de comunicație care va fi interceptată;
- tipul de informații care vor fi obținute;
- identitatea persoanelor sau categoriile de persoane care constituie ținta investigării;
- identitatea persoanelor, dacă e cunoscută, ale căror comunicații vor fi interceptate;
- o descriere generală a locului, dacă e cunoscut, în care se va face uz de mandat;
- perioada pentru care se solicită mandatul;
- detaliile oricărei cereri făcute anterior, care vizează o persoană identificată în actuala cerere – inclusiv data cererii anterioare, numele judecătorului căruia i-a fost adresată solicitarea și decizia luată de judecător în acel caz.

O bună practică pentru legislația care reglementează această chestiune este specificarea tipului de operațiuni care au nevoie de autorizare judiciară, precum și a autorității pe care o poate avea judecătorul de a limita sfera, durata și țintele unei operațiuni. Totodată, legislația trebuie să stabilească un necesar minim de informații care să stea la baza cererii de obținere a oricărui mandat (a se vedea Caseta 1).

În multe țări, pentru interceptarea comunicațiilor, este nevoie de un mandat judiciar. De exemplu, „Legea privind informațiile naționale” din Argentina impune serviciilor de informații ale țării să obțină autorizarea judiciară înainte de interceptarea comunicațiilor private de orice fel.[18]

Uneori, legea aplicabilă prevede ca cererile serviciilor de informații să fie examinate de judecători specializați. Canada, Franța, Africa de Sud și Spania, prin-

[17] Canadian Security Intelligence Service Act [Lege privind Serviciul Canadian pentru Informații de Securitate] (31 august 2004), R.S.C., 1985, Capitolul C-23, Secțiunea 21 (2) (disponibil la http://www.csis-scrs.gc.ca/pblctns/ct/cssct-eng.asp).

[18] Argentina, National Intelligence Law, Law 25520 of 2001 [Lege privind informațiile naționale, Legea 25520 din 2001], Titlul VI, Articolul 18.

tre altele, urmează această practică. Alternativ, unele țări au înființat instanțe speciale care să asigure autorizarea judiciară. Printre ele, se numără Curtea pentru Supravegherea Informațiilor Externe (FISC) din SUA, înființată prin „Legea privind supravegherea informațiilor externe” din 1978. Alcătuită din 11 judecători districtuali federali, care ocupă funcția eșalonat, pe termen de cel mult șapte ani ce nu poate fi reînnoit, FISC examinează solicitările de mandate pentru chestiuni legate de securitatea națională. Prin lege, a fost înființată Curtea de Apel pentru Supravegherea Informațiilor Externe care audiază recursurile guvernului la deciziile FISC.[19]

Uneori, acești judecători specializați și curțile în cauză au autoritatea de a verifica operațiunile de culegere de informații pe parcursul desfășurării lor. În Africa de Sud, „Legea pentru reglementarea interceptării comunicațiilor și a furnizării de informații asociate comunicațiilor,” din 2002, permite judecătorilor să ceară rapoarte scrise intermediare asupra progreselor făcute în vederea atingerii obiectivelor stabilite în mandat.[20] În acest fel, ei pot limita intruziunea colaterală asupra unor ținte ce nu au fost avute în vedere și pot să se asigure că metodele sub acoperire, intruzive, nu sunt folosite pe o perioadă mai lungă decât e necesar.

6. SUPRAVEGHEREA OPERAȚIUNILOR DE CULEGERE DE INFORMAȚII

Un complement important al autorizării este supravegherea, care include verificarea operațiunilor efectuate de serviciile de informații pentru a confirma că acestea au fost autorizate în mod corespunzător. Numai atunci când ambele măsuri de siguranță – autorizarea și supravegherea – sunt prezente, operațiunile de culegere a informațiilor pot fi considerate reglementate în mod real. (Pentru o discuție privind modul în care organismele de supraveghere gestionează reclamațiile împotriva serviciilor de informații, a se vedea Forcese – Instrumentul 9).

Supravegherea poate fi efectuată de numeroase entități diferite. Unele, precum instituțiile supreme de audit și instituțiile naționale de tip ombudsman, au

---

19 Web site-ul Centrului Judiciar Federal „Foreign Intelligence Surveillance Court” [„Curtea pentru Supravegherea Informațiilor Externe”] (disponibil la www.fjc.gov/history/home.nsf/page/courts_special_fisc.html).

20 Africa de Sud, Regulation of Interception of Communications and Provision of Communication-Related Information Act [Legea pentru reglementarea interceptării comunicațiilor și a furnizării de informații asociate comunicațiilor], Legea nr. 70 din 2002, în *Government Gazette*, Vol. 451, no. 24286 (22 ianuarie 2003), Secțiunea 24 (disponibil la www.info.gov.za/gazette/acts/2002/a70-02.pdf).

relevanță în virtutea mandatelor lor extinse. Altele, precum inspectorii generali și organismele specializate de supraveghere, dețin expertiză de specialitate, ceea ce vine în sprijinul mandatelor lor specifice. Cele mai multe țări distribuie supravegherea între mai multe entități cu jurisdicții ce se suprapun în diferite proporții.

6.1 ORGANISMELE PARLAMENTARE DE SUPRAVEGHERE

În cadrul sistemelor democratice de guvernare, parlamentele răspund pentru crearea cadrului legal în care funcționează organismele guvernamentale. Ele au și responsabilitatea de a monitoriza respectarea legilor pe care le adoptă. Aceste responsabilități se aplică și în cazul serviciilor de informații, la fel ca în cazul oricărei agenții guvernamentale.

Totuși, dat fiind că serviciile de informații diferă de celelalte agenții guvernamentale din mai multe puncte de vedere, parlamentele înființează, de regulă, comisii de supraveghere a serviciilor de informații pentru a monitoriza activitatea serviciilor și a recomanda revizuirea cadrului legal ce reglementează funcţionarea acestora. În ceea ce privește operațiunile de culegere de informații, comisiile respective au, de obicei, sarcina:

- să supravegheze utilizarea metodelor intruzive, sub acoperire;
- să monitorizeze elaborarea bugetului și utilizarea fondurilor;
- să analizeze cadrul legal, pentru a se asigura că acesta conține măsuri de siguranță suficiente pentru protecția drepturilor omului;
- să se asigure că serviciile de informații respectă cadrul legal.

În plus, legea de reglementare poate împuternici comisiile parlamentare să verifice operațiunile sub acoperire, intruzive, de culegere a informațiilor. În mod special, comisiile de supraveghere pot avea un rol esențial în asigurarea aplicării corecte a procedurilor de autorizare. De pildă, „Legea privind informațiile naționale” din Argentina împuternicește Comisia mixtă pentru supravegherea agențiilor și activităților de informații să oblige la pregătirea (și prezentarea în fața comisiei a) rapoartelor care enumeră „interceptările și înregistrările convorbirilor telefonice, efectuate într-o anumită perioadă.”[21] Comisia poate folosi apoi această listă pentru a verifica modul de utilizare a tehnicilor speciale de investigare în raport cu aprobările acordate. Astfel, ea poate confirma că procedurile de autorizare sunt utilizate corect; ca exemplu, a se vedea Caseta 2.

[21] Argentina, National Intelligence Law, Law 25520 of 2001 [Lege privind informațiile naționale, Legea 25520 din 2001], Titlul VI, Articolul 34II.

Caseta 2: Supravegherea parlamentară a culegerii de informații în Germania

În Germania, utilizarea metodelor intruzive de culegere a informațiilor este supravegheată de Comisia specială de control parlamentar.

Legea impune executivului să furnizeze comisiei de control rapoarte privind utilizarea metodelor intruzive, „la intervale nu mai mari de șase luni.” Pe baza acestor rapoarte periodice, comisia pregătește un raport anual pentru Bundestag asupra naturii și sferei de aplicare a metodelor intruzive folosite în temeiul legii.[22]

Totodată, pe lângă această funcție de monitorizare, legea acordă comisiei de control un rol de autorizare. Serviciul Federal de Informații (un serviciu de informații externe) trebuie să obțină aprobarea comisiei de control înainte de a putea intercepta traficul de telecomunicații internaționale care e transmis sub „formă de pachet” și care poate avea legătură cu Germania sau cu cetățenii germani. Este vorba despre interceptări pe baza unor cuvinte-cheie, ce nu vizează comunicări anume.[23]

Calitatea de membru într-o comisie parlamentară de supraveghere nu impune, în general, vreo expertiză în materie de intelligence. Totuși, așa cum a remarcat un membru al Congresului SUA, pentru a face aprecieri corecte, membrii comisiei trebuie să se familiarizeze cu informațiile care sunt produse și cu metodele folosite în acest scop.[24]

6.2 ORGANISMELE SPECIALIZATE DE SUPRAVEGHERE

Organismele specializate de supraveghere a serviciilor de informații sunt entități independente, ale căror membri și staff au o expertiză remarcabilă în domeniul intelligence (a se vedea Born și Geisler Mesevage – Instrumentul 1). Unul din cele mai obișnuite tipuri de organisme specializate de supraveghere este cel al inspectorilor generali. Deși funcțiile și responsabilitățile lor variază

[22] Germania, Act Restricting the Privacy of Correspondence, Posts and Telecommunications [Lege privind restricționarea caracterului privat al corespondenței, poștei și telecomunicațiilor] (26 iunie 2001), în *Federal Law Gazette I*, p. 1254, revizuită 2298, ultima dată amendată de Articolul 1 al Legii din 31 iulie 2009, *Federal Law Gazette I*, p. 2499, Secțiunea 14.

[23] Ibid., Secțiunea 5.

[24] L. Britt Snyder, *Sharing Secrets with Lawmakers:Congress as a User of Intelligence* [*Secrete împărtășite legislatorilor: Congresul ca utilizator de intelligence*] (Washington: Central Intelligence Agency, februarie 1997) p. 49 (disponibil la https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/sharing-secrets-withlawmakers-congress-as-a-user-of-intelligence/toc.htm).

de la un stat la altul, inspectorii generali sunt în mod normal entități independente, autorizate să primească reclamații privind legalitatea conduitei serviciilor de informații și să acționeze în consecință. Mandatele lor includ de obicei dreptul de a efectua investigații asupra modului de utilizare a tehnicilor speciale de investigare și a metodelor de culegere a informațiilor sub acoperire. În unele țări, precum SUA și Canada, ei funcționează în cadrul serviciilor de informații. În altele, precum Africa de Sud, sunt independenți, funcționând în afara acestor servicii.

Inspectorul general pentru informații din Africa de Sud are următoarele responsabilități principale de supraveghere:[25]

- să verifice activitățile serviciilor de informații pentru a stabili dacă au o conduită legală și dacă performanțele lor sunt reale.
- să certifice legalitatea operațiunilor efectuate de serviciile de informații în fața executivului și a populației din Africa de Sud;
- să funcționeze ca o instituție de tip ombudsman în ceea ce privește reclamațiile împotriva serviciilor de informații, făcute de oficiali guvernamentali și de orice alte persoane.

Spre deosebire de cele de mai sus, Belgia (a se vedea Caseta 3), Germania (a se vedea Caseta 4), Norvegia și Olanda folosesc organisme specializate pentru a-și supraveghea serviciile de informații. În privința operațiunilor de culegere de informații, aceste organisme specializate îndeplinesc următoarele sarcini:

- se asigură că operațiunile respectă cadrul legal, procedurile interne ale serviciilor în cauză și politicile executivului;
- monitorizează eficacitatea operațională și fac recomandări pentru îmbunătățirea ei;
- gestionează reclamațiile privind utilizarea ilegală a tehnicilor speciale de investigare, înaintate de oficiali guvernamentali și de orice persoane.

Pentru a fi eficace în supravegherea modului de culegere a informațiilor, un organism specializat de supraveghere trebuie să dispună de un mandat care să îi permită să fie proactiv. Mai precis, el trebuie să fie împuternicit să desfășoare investigații din proprie inițiativă și să aibă acces la o gamă largă de

[25] Imtiaz Fazel, „Who shall guard the guards? Civilian oversight and the Inspector General of Intelligence” [„Cine păzește paznicii? Supravegherea civilă și Inspectorul General pentru Informații”], în *To spy or not to spy? Intelligence and democracy in South Africa*, ed. Lauren Hutton (Pretoria: Institute for Security Studies, 2009), pp. 35–36.

informații deținute de servicii, fie ele clasificate sau nu. În schimb, el trebuie să ofere persoanelor care pretind că le-au fost încălcate drepturile posibilitatea de a face apel; și trebuie să pregătească rapoarte periodice pentru parlament. (Versiunile editate ale acestor rapoarte trebuie să fie difuzate public în vederea promovării transparenței.)

Caseta 3: Comisia Permanentă pentru Verificarea Agențiilor de Informații din Belgia

Un exemplu de organism specializat de supraveghere este Comisia Permanentă pentru Verificarea Agențiilor de Informații din Belgia, înființată prin „Legea pentru reglementarea verificării poliției și serviciilor de informații și a Unității de Coordonare pentru Evaluarea Amenințărilor." Comisia este mandatată să supravegheze funcționarea celor două servicii de informații din Belgia, precum și Unitatea de Coordonare pentru Evaluarea Amenințărilor. Supravegherea efectuată de comisie se axează pe legalitatea și eficacitatea activităților desfășurate de serviciile de informații, precum și pe coordonarea comunității de informații și de securitate. Pentru a face față acestor responsabilități, comisia este împuternicită să „investigheze activitățile și metodele serviciilor de informații," inclusiv modalitățile prin care serviciile culeg informații.[26]

În 2010, comisia a primit sarcina de a supraveghea utilizarea de către serviciile de informații a metodelor intruzive de culegere a informațiilor, adoptate recent. Comisia evaluează fiecare operațiune intruzivă de urmărire și poate ordona renunțarea la ea (și distrugerea informațiilor culese) dacă nu respectă legea.[27] Mai mult, această comisie e autorizată să gestioneze „reclamațiile și denunțurile … referitoare la modul de operare, intervenția, acțiunea sau lipsa de acțiune a serviciilor de informații."[28]

---

[26] Belgia, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment [Lege pentru reglementarea verificării poliției și serviciilor de informații și a Unității de Coordonare pentru Evaluarea Amenințărilor] (18 iulie 1991); a se vedea, de asemenea, site-ul Comisiei Permanente pentru Verificarea Agențiilor de Informații din Belgia (disponibil la www.comiteri.be).

[27] Belgia, Loi relative aux méthodes de recueil des données par les services de renseignement et de sécurité [Lege privind metodele de culegere a datelor de către serviciile de informații și de securitate] (4 februarie 2010).

[28] Belgia, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment [Lege pentru reglementarea verificării poliției și serviciilor de informații și a Unității de Coordonare pentru Evaluarea Amenințărilor] (18 iulie 1991), Articolul 34.

Caseta 4: Comisia G10 din Germania

Organismul specializat de supraveghere care monitorizează culegerea de informații în Germania este Comisia G10. Acest organism e alcătuit din patru membri, dintre care unul este judecător, și poate include parlamentari. Deși membrii comisiei sunt numiți de Comisia specială de control parlamentar, independența lor în funcție e garantată prin lege. Una dintre atribuțiile lor principale este de a decide cu privire la admisibilitatea și necesitatea folosirii metodelor intruzive de culegere a informațiilor. În consecință, legea prevede ca guvernul german să aducă lunar la cunoștința membrilor comisiei viitoarele operațiuni care vor utiliza metode intruzive de investigare. În cazul în care membrii comisiei declară că oricare din aceste metode nu e necesară sau admisibilă, guvernul va trebui să-și revoce autorizarea pentru operațiunile respective.[29]

Comisia G10 deține și o funcție de gestionare a reclamațiilor. Ea poate examina reclamații legate, inter alia, de utilizarea metodelor intruzive de culegere a informațiilor și poate decide dacă aceste reclamații oferă un temei suficient pentru a limita capacitatea serviciilor de informații de a folosi astfel de metode.[30]

7. CONCLUZII

Instrumentul de față a examinat cazurile și modul în care trebuie să li se permită serviciilor de informații să limiteze drepturile omului pentru a-și atinge obiectivele de securitate. Cu alte cuvinte, a analizat întrebarea: Când se pot folosi resurse publice pentru a limita drepturile indivizilor? În cazul unei asemenea întrebări, fundamentală este relația dintre cetățeni și guvernul lor. Oricare ar fi răspunsul la care ajunge o societate, este întotdeauna necesar un sistem riguros și clar definit de autorizări și de supraveghere pentru a se asigura menținerea conduitei agenților de informații în parametrii legii care le reglementează.

Supravegherea operațiunilor de culegere de informații e deosebit de importantă, deoarece, în țările democratice, o culegere eficace de informații depinde de legitimitatea instituțională, de o guvernare credibilă și, în cele din urmă, de încrederea publică. Aceste condiții pot fi întrunite doar dacă activitățile serviciilor de informații se fundamentează pe și respectă cadrul le-

[29] Ibid., Secțiunea 15.

[30] Germania, Act Restricting the Privacy of Correspondence, Posts and Telecommunications [Lege privind restricționarea caracterului privat al corespondenței, poștei și telecomunicațiilor] (Legea G10), (26 iunie 2001), în *Federal Law Gazette I*, p. 1254, revizuită 2298, ultima dată amendată de Articolul 1 al Legii din 31 iulie 2009, *Federal Law Gazette I*, p. 2499, Secțiunea 15.

gal ce protejează drepturile omului și dacă serviciile își însușesc principiile democratice ale deschiderii, transparenței și responsabilității. Pe aceste baze, și numai pe aceste baze, poate fi asigurată utilizarea legitimă a metodelor sub acoperire, intruzive.

8. RECOMANDĂRI

- Situațiile în care este permisă folosirea metodelor de investigare ce limitează drepturile omului, inclusiv dreptul la viață privată, trebuie să fie clar definite în cadrul legal care reglementează funcționarea serviciilor de informații.
- Cadrul legal trebuie să specifice motivele pertinente pentru utilizarea metodelor sub acoperire, intruzive, de culegere a informațiilor, admițând faptul că acestea trebuie folosite numai atunci când corespund ca însemnătate obiectivului avut în vedere și când nicio altă metodă nu ar fi suficientă.
- Cadrul legal trebuie să stabilească proceduri clare de autorizare, care să reglementeze folosirea metodelor sub acoperire, intruzive, de culegere a informațiilor. Cu cât este mai mare nivelul intruziunii, cu atât trebuie să fie mai înalt nivelul de autorizare.
- Cadrul legal trebuie să impună autorizarea judiciară pentru utilizarea pe plan intern a metodelor sub acoperire, intruzive, de culegere a informațiilor. El va stabili, de asemenea, proceduri pentru desemnarea judecătorilor autorizați să acorde astfel de aprobări și va preciza de ce criterii trebuie să se țină seama la evaluarea cererilor respective din partea guvernului.
- Cadrul legal trebuie să instituie mecanisme eficace de supraveghere, care să monitorizeze utilizarea metodelor sub acoperire, intruzive, de culegere de informații, prin intermediul comisiilor parlamentare, al organismelor specializate de supraveghere sau al ambelor tipuri de entități.

INSTRUMENTUL 6

Supravegherea utilizării datelor cu caracter personal

Ian Leigh



6

Supravegherea utilizării datelor cu caracter personal

Ian Leigh

1. INTRODUCERE

Acest instrument studiază modul în care organismele de supraveghere se pot asigura că serviciile de informații folosesc datele cu caracter personal în conformitate cu legea care reglementează funcționarea respectivelor servicii. El urmărește să explice rolul deținut de organismele de supraveghere în examinarea modului în care serviciile de informații stochează, accesează și transferă aceste date. Nu se ocupă de culegerea informațiilor de către serviciile respective (abordată de Hutton – Instrumentul 5) sau de comunicarea de date cu caracter personal unor parteneri interni și externi (abordată de Roach – Instrumentul 7).

Subiectul examinat în instrumentul de față include: riscurile care decurg din utilizarea datelor cu caracter personal de către serviciile de informații; cadrul legal corespunzător pentru reglementarea acestei utilizări; și mijloacele prin care se face supravegherea ei. Capitolul se încheie cu un scurt rezumat al principiilor-cheie pentru adoptarea legislației cu privire la utilizarea datelor cu caracter personal de către serviciile de informații.

În conformitate cu practica internațională larg răspândită, acest instrument va folosi termenul de *date cu caracter personal* pentru a înțelege „orice informații referitoare la o persoană identificată sau identificabilă («subiectul datelor»).” [1]

[1] Această definiție apare în Articolul 2 al Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [Convenția Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal] și în Secțiunea 1(b) a lucrării Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [Liniile directoare ale Organizației pentru Cooperare și Dezvoltare Economică (OCDE), privind protecția

2. RISCURI ÎN UTILIZAREA DATELOR CU CARACTER PERSONAL DE CĂTRE SERVICIILE DE INFORMAȚII

Serviciile de informații au motive legitime, decurgând din mandatul lor legal, de a culege, stoca, prelucra și dezvălui date cu caracter personal. Persoanele la care se referă datele pot fi ținte legitime, deoarece, de pildă, sunt suspectate de implicare în spionaj sau terorism. Nevoia de culegere a unor astfel de informații variază de la o țară la alta și de la un serviciu la altul în funcție de responsabilitățile legale concrete ale fiecărui serviciu.

Există, totuși, un pericol constant de a mări excesiv volumul datelor cu caracter personal care se culeg. De exemplu, procesul prin care se stabilește dacă o persoană suspectă e angajată în activități teroriste are în vedere posibilitatea ca informațiile culese să conducă la o concluzie negativă. Evident, într-o astfel de situație, culegerea inițială de informații nu poate fi considerată nepotrivită; dar, odată ce serviciul a stabilit că persoana nu e implicată, el nu ar trebui să continue activitatea de culegere (sau, discutabil, chiar să rețină și să folosească informațiile pe care le-a obținut). Mai mult, procedând astfel, există riscul ca serviciul să fie tentat să culeagă informații din cercuri din ce în ce mai largi – de exemplu, despre asociații persoanei suspecte sau despre organizația societății civile din care fac parte aceștia. O astfel de tendință poate induce frică, determinându-i pe indivizi să se teamă să facă parte din organizații civile legale, precum sindicatele, partidele politice separatiste și grupurile ecologiste sau anti-nucleare. De asemenea, există și un pericol mai general, ca datele cu caracter personal stocate în dosarele unui serviciu de informații să fie incorect folosite – de oficiali din statele în tranziție, spre exemplu, pentru a șantaja oponenții politici sau a tempera jurnaliștii.

Uneori, se susține că simpla stocare, analizarea și păstrarea datelor de către serviciile de informații au caracter benign. În vreme ce culegerea datelor cu caracter personal prezintă mai multe riscuri evidente (a se vedea Hutton – Instrumentul 5), stocarea lor este potențial dăunătoare, deoarece aceste date sunt strâns legate de autonomia personală. Controlul pe care persoanele îl exercită asupra propriei lor vieți – în special alegerile pe care le fac în privința detaliilor personale (cui, în ce măsură și în ce scop optează să le dezvăluie) – este erodat atunci când agențiilor guvernamentale li se permite să adune date cu caracter personal din mai multe surse.

---

vieții private și fluxurile transfrontaliere de date personale]. O definiție similară apare în Articolul 2(a) al European Union Directive 95/46/EC [Directiva Uniunii Europene 95/46/EC]; totuși, această directivă nu se aplică la activitățile ce țin de securitatea de stat (a se vedea Articolul 3.2).

Prin strângerea unor informații personale despre indivizi, serviciile de informații dobândesc, într-o oarecare măsură, control asupra subiecților acelor informații. În cel mai rău caz, datele cu caracter personal, deținute de servicii, pot fi utilizate necorespunzător pentru a exercita presiuni asupra politicienilor sau jurnaliștilor. Însăși cunoașterea faptului că serviciile dețin date cu caracter personal poate fi perturbatoare din punct de vedere psihologic pentru persoanele vizate, chiar dacă nicio dezvăluire dăunătoare nu va avea loc vreodată. În mod similar, participarea în cadrul societății civile poate fi descurajată de cunoașterea (sau suspiciunea constantă) că datele despre anumite forme de activism politic, industrial și social sunt păstrate în dosare de securitate.

Ținând seama de nevoia, declarată adeseori, de a păstra informațiile de securitate pe perioade lungi de timp, perspectiva unui prejudiciu poate afecta persoanele în cauză mulți ani sau multe decenii. Informațiile privind activitățile din tinerețe, de pildă, pot fi păstrate în unele cazuri și atunci când persoanele respective au o vârstă înaintată, chiar dacă viața lor ulterioară nu oferă motive pentru a fi considerate drept un risc la adresa securității.

Mai mult, datele cu caracter personal deținute de serviciile de informații pot fi parțiale, inexacte sau depășite. În situații extreme, este posibil să fi fost obținute de la surse care doreau să facă rău persoanei respective din cauza unor animozități personale sau din invidie. În mod similar, surse motivate printr-o răsplată financiară pot avea tendința să exagereze sau să născocească fapte atunci când furnizează informații despre anumite persoane.

Alte riscuri legate de stocarea datelor cu caracter personal includ capacitatea fără precedent a unor servicii de informații de a corela, printr-un acces privilegiat, informații despre un individ, conținute în baze de date ale organismelor de aplicare a legii, medicale și ale fiscului, altminteri distincte.

Desigur, riscurile nu se sfârșesc odată cu stocarea, ordonarea și analiza datelor cu caracter personal. Există și riscuri asociate cu utilizarea lor. Unele utilizări sunt legitime (așa cum este verificarea din punct de vedere al securității), în vreme ce altele sunt mai puțin demne de laudă (precum conturarea unui profil rasial sau religios ori exercitarea, pe ascuns, a unei influențe asupra unei persoane). O dezvăluire cu autor necunoscut a unor date personale în mass-media, de exemplu, poate provoca persoanei respective prejudicii și pierderea unor oportunități. Statutul său profesional poate fi afectat, spre exemplu, prin refuzarea acordării sau pierderea certificatului de securitate; și, la un nivel mai general, reputația sa poate fi lezată. În mod similar, dezvăluirea unor date neîntemeiate sau inexacte unor guverne străine poate duce la pierderea oportunităților de a călători sau poate avea consecințe chiar mult mai grave (a se vedea Roach – Instrumentul 7).

Serviciile de informații sunt puternic interesate să se asigure că informațiile pe care le dețin despre anumite ținte legitime sunt corecte, exacte și actualizate. Eficacitatea și reputația unui serviciu pot fi afectate dacă acesta dezvăluie, dă un aviz ori acționează pe baza unor informații greșite, incomplete sau depășite. Totuși, există anumite riscuri inerente activității din domeniul intelligence, care întăresc nevoia de control și supraveghere externe cu privire la procedurile de gestionare a informațiilor. Îndeosebi imperativul anticipării viitoarelor riscuri de securitate poate încuraja serviciile să culeagă informații în exces despre un număr tot mai mare de persoane. Schimbările tehnologice, așa cum este perfecționarea activității de căutare de date, pot stimula, în același timp, culegerea și stocarea unor cantități vaste de date cu caracter personal, precum datele privind traficul pe e-mail, căutările pe web-site-uri, rezervările la curse aeriene și tranzacțiile financiare.

3. CADRUL LEGAL PENTRU UTILIZAREA DATELOR CU CARACTER PERSONAL DE SERVICIILE DE INFORMAȚII

Dreptul la viață privată este protejat conform normelor de drept în materia drepturilor omului, consacrate de cele mai importante tratate internaționale.[2] Totuși, din rațiuni de relevanță și utilitate practică, instrumentul de față se va concentra asupra normelor privind drepturile omului, aplicabile în Europa, în special cele stabilite în *Convenția europeană a drepturilor omului* (ECHR), care sunt cele mai avansate. Deși acest capitol se axează pe dreptul la viață privată, culegerea și utilizarea datelor cu caracter personal de către agențiile de informații poate avea și un impact indirect asupra altor drepturi ale omului, așa cum sunt dreptul la liberă exprimare și acela privind libera asociere.

Articolul 8 al ECHR, care se aplică celor 47 de state membre ale Consiliului Europei, stipulează:

> 1. *Orice persoană are dreptul la respectarea vieţii sale private şi de familie, a domiciliului său şi a corespondenţei sale.*

---

[2] Articolul 17 al *International Covenant on Civil and Political Rights* [*Convenția internațională cu privire la drepturile civile și politice*] stabilește că: „1. Nimeni nu va putea fi supus vreunor imixtiuni arbitrare sau ilegale în viața particulară, în familia, domiciliul sau corespondența sa, nici la atingeri ilegale aduse onoarei și reputației sale. 2. Orice persoană are drept la protecția legii împotriva unor asemenea imixtiuni sau atingeri.” Articolul 12 din *Universal Declaration of Human Rights* [*Declarația universală a drepturilor omului*] precizează că „Nimeni nu va fi supus la imixtiuni arbitrare în viața sa personală, în familia sa, în domiciliul sau în corespondența sa, nici la atingeri aduse onoarei și reputației sale. Orice persoană are dreptul la protecție din partea legii împotriva unor asemenea imixtiuni sau atingeri.”

[Curtea Europeană a Drepturilor Omului (CEDO) a interpretat această prevedere ca incluzând apelurile telefonice și celelalte mijloace de comunicare electronică.]

2. Nu este admis amestecul unei autorităţi publice în exercitarea acestui drept decât în măsura în care acest amestec este prevăzut de lege şi dacă constituie o măsură care, într-o societate democratică, este necesară pentru securitatea naţională, siguranţa publică, bunăstarea economică a ţării, apărarea ordinii și prevenirea faptelor penale, protejarea sănătăţii sau a moralei, ori protejarea drepturilor şi libertăţilor altora.

De asemenea, *Carta drepturilor fundamentale a Uniunii Europene* este relevantă prin prevederile explicite referitoare la protecția datelor cu caracter personal, care sunt obligatorii pentru statele membre ale Uniunii Europene (UE). Articolul 8 afirmă:

1 Orice persoană are dreptul la protecţia datelor cu caracter personal care o privesc.

2. Asemenea date trebuie tratate în mod corect, în scopurile precizate şi pe baza consimţământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut de lege. Orice persoană are dreptul de acces la datele colectate care o privesc, precum şi dreptul de a obţine rectificarea acestora.

3. Respectarea acestor norme se supune controlului unei autorităţi independente.

Mai mult, în conformitate cu Articolul 52.1 al Cartei:

Orice restrângere a exerciţiului drepturilor şi libertăţilor recunoscute prin prezenta cartă trebuie să fie prevăzută de lege şi să respecte substanţa acestor drepturi şi libertăţi. Prin respectarea principiului proporţionalităţii, pot fi impuse restrângeri numai în cazul în care acestea sunt necesare şi numai dacă răspund efectiv obiectivelor de interes general recunoscute de Uniune sau necesităţii protejării drepturilor şi libertăţilor celorlalţi.

Totuși, dat fiind că prevederile *Cartei drepturilor fundamentale* nu au produs încă jurisprudență, capitolul de față se va axa în principal asupra ECHR.

CEDO a constatat că dosarele guvernamentale de securitate, ce conțin date cu caracter personal, se încadrează în mod clar în sfera protejată a vieții private, enunțată la Articolul 8 al ECHR. Curtea a mai constatat, în multe cazuri, că activitatea de culegere, stocare și comunicare a datelor cu caracter personal de către un serviciu de informații constituie „o ingerință” în privința dreptului la viață privată – care este permisă doar în temeiul criteriilor stricte, prevăzute la Articolul 8.2. Constatările Curții se aplică nu numai la dezvăluirea informațiilor în atenția altor agenții guvernamentale, dar și la utilizarea lor pentru verifica-

rea internă și emiterea certificatului de securitate.[3] În decizia luată în cazul Rotaru versus România (2000), care se referă la dosarele de securitate deținute de serviciile de informații, Curtea a constatat că:

> atât stocarea de către o autoritate publică a datelor referitoare la viața privată a unei persoane, cât și utilizarea lor și refuzul de a acorda o ocazie pentru a li se dovedi netemeinicia echivalează cu ingerința în dreptul la viață privată, consacrat în Articolul 8.1 al Convenției.[4]

3.1 LIMITĂRI ADMISIBILE ALE DREPTULUI LA VIAȚĂ PRIVATĂ

Pentru ca stocarea și utilizarea datelor cu caracter personal de către un serviciu de informații să fie conforme cu ECHR, trebuie să se respecte criteriile stabilite în Articolul 8.2. Și anume, utilizarea trebuie să fie „în conformitate cu legea,” „necesară într-o societate democratică” și „în interesul securității naționale.”

Condiția „în conformitate cu legea” impune un criteriu stringent. Dacă acest criteriu nu poate fi respectat, se încalcă Articolul 8, indiferent de interesele mai mari care se află în joc.

Astfel, cerința privind legalitatea impune parlamentarilor să alcătuiască o bază legală solidă pentru folosirea datelor cu caracter personal de către serviciile de informații.

CEDO a interpretat cerința „în conformitate cu legea” ca având semnificația că orice restrângere a dreptului la viață privată trebuie „să aibă o bază în dreptul intern” și să treacă testul „calității legii,” ceea ce înseamnă, potrivit definiției Curții, că legea trebuie să fie „accesibilă pentru persoana interesată, care, în plus, trebuie să-i poată prevedea consecințele pentru ea însăși, și (să fie) compatibilă cu statul de drept.” [5]

Aplicând acest test, CEDO a constatat nerespectări ale Articolului 8 acolo unde nu există legi referitoare la serviciile de informații sau acolo unde o asemenea lege există, dar nu cuprinde prevederi care să reglementeze culegerea și stocarea datelor cu caracter personal.[6] Mai mult, conform testului privind „calitatea legii,” o astfel de lege „trebuie să fie redactată în termeni suficient de clari pentru a oferi cetățenilor o indicație adecvată asupra circumstanțelor în care

---

3 Curtea Europeană a Drepturilor Omului (CEDO) – *Leander v. Sweden* [*Leander versus Suedia*], Nr. 9248/81, 1987.

4 *Rotaru v. Romania* [*Rotaru versus România*], Nr. 28341/95, CEDO, 2000, Paragraful 46.

5 *Weber and Saravia v. Germany* [*Weber și Saravia versus Germania*], Nr. 54934/00, CEDO, 2006, Paragraful 84.

6 *R. V. v. The Netherlands* [R.V. versus Olanda], Nr. 14084/88, CEDO, 1991.

Caseta 1: Testul „calității legii" în practică

În cazul *Rotaru versus România*,[7] Curtea Europeană a Drepturilor Omului a analizat legislația română care stabilea reguli referitoare la dosarele de securitate deținute de guvern. Curtea a reținut că legea era insuficient de clară în descrierea circumstanțelor în care putea fi folosită – mai precis, ce utilizări puteau fi date informațiilor personale din dosare – și nici nu stabilea vreun mecanism de monitorizare a modului de utilizare a informațiilor.

Curtea a mai constatat că legea avea lacune, deoarece nu „indica" cu o claritate rezonabilă sfera de cuprindere a împuternicirii acordate guvernului român. Altfel spus, legea nu limita exercitarea de către guvern a puterii de a aduna, înregistra și arhiva informații personale în dosare secrete. Mai precis, legea nu definea tipul de informații ce puteau fi înregistrate, categoriile de persoane împotriva cărora puteau fi luate măsuri de urmărire, circumstanțele în care asemenea măsuri puteau fi luate, precum și procedurile de urmat. Și nici nu cuprindea vreo limitare a perioadei de timp pentru care informațiile puteau fi păstrate.[8]

În ceea ce privește arhivele de securitate deținute de serviciile de informații de dinaintea Revoluției, legea permitea ca aceste arhive să fie consultate, însă nu includea „prevederi explicite, detaliate, referitoare la persoanele autorizate să consulte dosarele, natura dosarelor, procedurile de urmat sau modul în care puteau fi întrebuințate informațiile astfel obținute." [9]

[legea poate fi utilizată]." [10] În plus, deoarece „nu se permite ca aplicarea în practică a măsurilor de urmărire secretă a comunicațiilor să fie examinată de persoanele interesate sau de publicul larg," legile care reglementează culegerea de date cu caracter personal nu trebuie să permită „ca împuternicirea legală acordată executivului sau unui judecător să se exprime în termenii unei puteri nelimitate" și, în consecință, respectivele legi trebuie „să indice sfera de cuprindere a împuternicirii acordate … și maniera în care este întrebuințată, cu suficient de multă claritate, încât să asigure persoanei în cauză o protecție corespunzătoare împotriva unor ingerințe arbitrare." [11]

În evaluarea unor astfel de legi, Curtea verifică dacă ele explică suficient de clar, *inter alia*, procedurile de urmat pentru examinarea, utilizarea și stocarea datelor obținute, precauțiile ce trebuie luate atunci când datele sunt comuni-

---

7 *Rotaru v. Romania* [*Rotaru versus România*], Nr. 28341/95, CEDO, 2000.

8 Ibid., Paragraful 57.

9 Ibid.

10 *Weber and Saravia v. Germany* [*Weber și Saravia versus Germania*], Nr. 54934/00, CEDO, 2006, Paragraful 93.

11 Ibid., Paragraful 94.

cate altor părți și circumstanțele în care înregistrările obținute prin urmărire pot fi sau trebuie să fie distruse.[12]

Un caz recent ce implică guvernul rus ilustrează principiile enunțate.[13] Curtea a constatat că înregistrarea unui activist pentru drepturile omului într-o bază de date de urmărire secretă a încălcat Articolul 8 al ECHR. Dat fiind că baza de date a fost creată în temeiul unui ordin ministerial nepublicat, care nu era accesibil publicului, membrii acestuia nu puteau cunoaște de ce anumiți indivizi erau înregistrați în acea bază de date, ce tip de informații erau stocate, cum erau stocate, pentru câtă vreme, cum urma să fie folosite și cine urma să le controleze.

Totuși, testul privind „calitatea legii” ia în considerare preocupările legitime legate de securitate. În contextul verificării de securitate, de exemplu, „previzibilitatea,” ca parte a testului, nu impune solicitanților să fie capabili să prevadă întregul proces (altminteri, acesta ar putea fi cu ușurință evitat). Mai curând, legea de autorizare trebuie să conțină numai o descriere generală a practicii.[14]

Odată depășite obstacolele privind claritatea, accesibilitatea și previzibilitatea din testul „calității legii,” ECHR impune o analiză a scopului și necesității ingerinței în viața privată. Ceea ce atrage după sine o evaluare a proporționalității – cu alte cuvinte, a stabili dacă ingerința este excesivă, chiar atunci când se ține seama de scopul legitim de protejare a securității naționale. De pildă, într-un caz recent, CEDO a constatat că guvernul suedez a încălcat Articolul 8 al ECHR atunci când a reținut date cu caracter personal într-un dosar de securitate pe o perioadă care a depășit 30 de ani. Ținând cont de natura și vechimea informațiilor, Curtea nu a acceptat argumentul apărării, potrivit căruia decizia de a continua stocarea informațiilor era susținută de rațiuni pertinente și suficiente privind securitatea națională.[15]

Atunci când analizează dacă o ingerință în viața privată este „necesară într-o societate democratică,” Curtea ia în considerare măsurile de siguranță care au fost stabilite pentru a supraveghea stocarea și utilizarea datelor cu caracter

12 A se vedea, de exemplu, analiza detaliată a legii referitoare la Comisia germană G10 în *Weber and Saravia v. Germany* [*Weber și Saravia versus Germania*], decizia de admisibilitate nr. 54934/00, CEDO, 2006.

13 *Shimovolos v. Russia* [*Shimovolos versus Rusia*], Nr. 30194/09, CEDO, 2011.

14 *Leander v. Sweden* [*Leander versus Suedia*], Nr. 9248/81, CEDO, 1987.

15 *Segerstedt-Wiberg and Others v. Sweden* [*Segerstedt-Wiberg și alții versus Suedia*], Nr. 62332/00, CEDO, 2006.

personal – în special cele care implică organismele independente.[16] Acolo unde nu există măsuri de siguranță care să permită unei persoane să-și protejeze dreptul la viață privată, Curtea va constata o încălcare a Articolului 8. În cazul *Turek versus Slovacia* (2006), de exemplu – un caz în care solicitantul a reclamat că a fost înregistrat drept colaborator al fostei agenții de securitate din Cehoslovacia comunistă, i s-a eliberat un certificat de securitate în acest sens și acțiunea sa de contestare a înregistrării a fost respinsă – Curtea a constatat că absența unei proceduri prin care solicitantul să poată acționa pentru a-și proteja dreptul la viață privată încălca Articolul 8.[17]

Chiar și atunci când o astfel de procedură este prevăzută în lege, amânarea excesivă a răspunsului la solicitări ale unor persoane de a avea acces la informațiile care le privesc poate fi considerată o încălcare a dreptului respectiv (deoarece măsurile de siguranță nu sunt eficace). De pildă, în cazul *Haralambie versus România* (2009), Curtea a constatat că întârzierea de șase ani cu care guvernul român a permis solicitantului accesul la dosarul său personal de securitate, alcătuit în vremea regimului anterior, comunist, a încălcat drepturile acestuia în temeiul Articolului 8 al ECHR.[18]

Prin urmare, este necesar să se precizeze limite legale clare pentru culegerea și utilizarea datelor cu caracter personal de către serviciile de informații, iar organismele de supraveghere trebuie să se asigure că serviciile respectă legile care reglementează gestionarea unor astfel de date. Raportorul special al Națiunilor Unite pentru promovarea și protejarea drepturilor omului și libertăților fundamentale în contextul combaterii terorismului a reiterat această necesitate în raportul său din 2010, prezentat Consiliului Națiunilor Unite pentru Drepturile Omului:

> Legislația disponibilă public evidențiază tipurile de date personale pe care le pot deține serviciile de informații și ce criterii se aplică pentru utilizarea, păstrarea, ștergerea și dezvăluirea unor asemenea date. Serviciilor de informații li se permite să păstreze datele personale care sunt strict necesare pentru scopul îndeplinirii mandatului lor.[19]

---

[16] *Leander v. Sweden* [*Leander versus Suedia*], Nr. 9248/81, CEDO, 1987, Paragrafele 52–57; a se vedea și *Rotaru v. Romania* [*Rotaru versus România*], Nr. 28341/95, CEDO, 2000, Paragraful 59.

[17] *Turek v. Slovakia* [Turek versus Slovacia], Nr. 57986/00, CEDO, 2006.

[18] *Haralambie v. Romania* [*Haralambie versus România*], Nr. 21737/03, CEDO, 2009.

[19] Consiliul Națiunilor Unite pentru Drepturile Omului, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight* [*Rapor-*

TABELUL 1: PRINCIPIILE CONSILIULUI EUROPEI PRIVIND PROTECȚIA DATELOR	
Principiu pentru protecția datelor	Cerințe
Calitatea datelor (Articolul 5)	Datele cu caracter personal supuse prelucrării automatizate trebuie să fie: a. obținute și prelucrate corect și legal; b. stocate în scopuri determinate și legitime și nu trebuie să fie utilizate într-un mod incompatibil cu aceste scopuri; c. adecvate, pertinente şi neexcesive în raport cu scopurile pentru care sunt stocate; d. exacte şi, acolo unde e necesar, actualizate; e. păstrate într-o formă care să permită identificarea subiecților în cauză pe o perioadă nu mai mare decât cea necesară scopurilor pentru care sunt stocate.
Securitatea datelor (Articolul 7)	Vor fi luate măsuri corespunzătoare de securitate pentru protecția datelor cu caracter personal, stocate în fişiere automatizate, împotriva distrugerii accidentale sau neautorizate ori a pierderii accidentale, precum şi împotriva accesării, modificării sau diseminării neautorizate a acestora.
Dreptul de a cunoaşte existența datelor cu caracter personal (Articolul 8)	Oricărei persoane i se va permite să afle despre existenţa unui fişier automatizat de date cu caracter personal, să cunoască scopurile principale ale acestuia, precum şi identitatea şi locul uzual de reşedinţă sau locul principal în care îşi desfăşoară activitatea gestionarul fişierului.
Dreptul de acces (Articolul 8)	Orice persoană va avea posibilitatea: • să obţină, la intervale rezonabile şi fără întârzieri sau cheltuieli excesive, confirmarea privind existenţa unor date cu caracter personal care o privesc, stocate într-un fişier automatizat, precum şi să i se comunice aceste date într-o formă inteligibilă; • să obţină, după caz, modificarea acestor date sau ştergerea lor, în situația în care au fost prelucrate fără a se respecta dispoziţiile din dreptul intern care aplică principiile de bază enunţate la art. 5 şi 6 ale acestei convenții.
Dreptul la o cale de atac (Articolul 8)	Orice persoană va avea posibilitatea: să dispună de o cale de atac dacă nu s-a dat curs unei cereri de confirmare sau, după caz, de comunicare, rectificare ori de ştergere, prevăzute la paragrafele b) şi c) din acest articol.

tul Raportorului special al Națiunilor Unite pentru promovarea și protejarea drepturilor omului și libertăților fundamentale în contextul combaterii terorismului: Compilație de bune practici privind cadrul și măsurile legale și instituționale, care asigură respectarea drepturilor omului de către agențiile de informații în contextul combaterii terorismului, inclusiv supravegherea acestora], United Nations Document A/HRC/14/46 (17 mai 2010), p. 21 (Practica 23).

3.2 PRINCIPII ALE PROTECȚIEI DATELOR

Convenția Consiliului Europei pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal [20] („Convenția pentru protecția datelor") stabilește principiile minime pentru statele membre în materie de protecție a datelor (a se vedea Tabelul 1). În temeiul acestei convenții, fiecare stat semnatar se angajează „să ia, în dreptul său intern, măsurile necesare pentru a pune în practică principiile de bază ale protecţiei de date" [21] și „să stabilească sancţiuni şi căi de atac adecvate în cazul violării dispoziţiilor de drept intern care dau efect principiilor de bază pentru protecţia datelor." [22] În plus, aspecte ale acestor principii – în special cele care se referă la prelucrarea corectă, consimțământ, autoritatea legală, accesul subiecților și rectificare – se pot regăsi în Articolul 8.2 al *Cartei drepturilor fundamentale a Uniunii Europene*.

Convenția pentru protecția datelor (la Articolul 11) stipulează că principiile pe care le conține trebuie înțelese ca standarde minime, ce pot fi suplimentate cu măsuri de protecție mai extinse.

Modul în care *Convenția pentru protecția datelor* tratează restricțiile în privința principiilor de protecţie a datelor este asemănător cu acela în care ECHR abordează restricțiile în privința dreptului la viață privată (amintite mai sus). Restricțiile trebuie să fie „prevăzute de legislație [a statelor semnatare]" și trebuie să reprezinte „o măsură necesară într-o societate democratică." [23]

---

[20] Consiliul Europei, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal], ETS No. 108 (Strasbourg, 28.I.1981). Convenția are la bază ampla influență a lucrării OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [Liniile directoare ale Organizației pentru Cooperare și Dezvoltare Economică (OCDE), privind protecția vieții private și fluxurile transfrontaliere de date personale] (23 septembrie 1980) disponibil la http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#part2). Liniile directoare ale OCDE stabilesc opt principii fundamentale privind protecția datelor, care se referă la limitarea activității de culegere, calitatea datelor, precizarea scopului, limitarea utilizării, măsuri de asigurare a securității, caracterul deschis, participare individuală și responsabilitate.

[21] Ibid., Articolul 4.

[22] Ibid., Articolul 10.

[23] Termenul de *măsură necesară* trebuie înțeles în contextul doctrinei proporționalității, enunțată în *Carta drepturilor fundamentale a Uniunii Europene.*

pentru a proteja un interes legitim, precum securitatea națională sau drepturile subiectului căruia îi aparțin datele respective.[24]

3.3 IMPORTANȚA LEGISLAȚIEI NAȚIONALE

Dat fiind faptul că drepturile omului pot fi serios prejudiciate în urma culegerii, folosirii şi dezvăluirii de către serviciile de informaţii a unor date cu caracter personal, se cuvine ca legislaţia accesibilă public să prevadă în mod democratic linii directoare pentru gestionarea și utilizarea unor asemenea date. Această practică are mai multe avantaje: ea stimulează o dezbatere politică profundă asupra scopului corect al activității serviciilor de informații, face ca procesul decizional să nu fie la discreția unui serviciu sau a executivului și atribuie serviciilor un mandat clar referitor la acțiunile care pot încălca drepturile omului.

Legislația care reglementează utilizarea datelor cu caracter personal de către serviciile de informații poate aborda una sau mai multe din următoarele teme:

- motivele admisibile și neadmisibile pentru prelucrarea datelor cu caracter personal;
- limitele în privința dezvăluirii datelor cu caracter personal;
- dezvăluirea publică a tipurilor de date stocate;
- accesul la datele cu caracter personal de către subiectul căruia îi aparțin;
- notificarea faptului că au fost culese date cu caracter personal;
- verificarea, revizuirea și ștergerea datelor cu caracter personal.

3.3.1 Motivele admisibile și neadmisibile pentru prelucrarea datelor cu caracter personal

Legislația din domeniu poate preciza tipurile de date cu caracter personal ce pot fi culese și reținute, precum și momentul în care un dosar care conține date cu caracter personal poate fi deschis (a se vedea Caseta 2). Recunoscând explicit principiul proporționalității, legislația germană corelează necesitatea culegerii de date cu gravitatea amenințării în cauză. Mai precis, ea impune serviciului intern de informații (Oficiul Federal pentru Protecția Constituției) să analizeze dacă informațiile dorite pot fi obținute din surse deschise sau prin folosirea unor mijloace care încalcă în mai mică măsură dreptul la viață pri-

[24] Consiliul Europei, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal], ETS No. 108 (Strasbourg, 28.I.1981), Articolul 9.

vată.[25] În același timp, o astfel de legislație poate reduce probabilitatea ca serviciile de informații să încalce drepturile omului prin interzicerea anumitor forme de conduită, precum atunci când își îndreaptă atenția spre anumite persoane pe baza caracteristicilor lor rasiale sau religioase ori a opiniilor lor politice.

Caseta 2: Limite în prelucrarea datelor cu caracter personal în diferite jurisdicții

Această casetă cuprinde prevederi din dreptul olandez și cel argentinian, care limitează prelucrarea datelor cu caracter personal de către serviciile de informații în temeiul unor criterii de neadmisibilitate.

Olanda [26]

„Serviciul General de Informații și Securitate poate prelucra numai date cu caracter personal referitoare la persoane:

a. care dau motive serioase de suspiciune ca fiind un pericol pentru sistemul democratic legal sau pentru securitate ori pentru alte interese vitale ale statului;
b. care au permis să fie investigate pentru obținerea unui certificat de securitate;
c. pentru care este necesar acest lucru în contextul investigațiilor privind alte țări;
d. despre care au fost obținute informații de către un alt serviciu de informații sau de securitate;
e. ale căror date sunt necesare în susținerea îndeplinirii corespunzătoare de către serviciu a îndatoririlor sale;
f. care sunt sau au fost angajate ale unui serviciu;
g. ale căror date e necesar să fie prelucrate în contextul elaborării unor analize ale riscurilor și amenințărilor, așa cum sunt menționate la Articolul 6, al doilea paragraf, litera e.”

Argentina [27]

„Nicio agenție de informații nu va … păstra date despre anumite persoane din motive de rasă, religie, acțiuni private și ideologie politică sau pe baza calității acestora de membri ai unor organizații de partid, sociale, sindicale, comunitare, cooperative, de asistență, culturale sau muncitorești, ori datorită activităților legale duse la îndeplinire în orice domeniu.”

---

[25] Germania, Federal Act on Protection of the Constitution [Legea federală privind protejarea Constituției] (20 decembrie 1990), în *Federal Law Gazette I*, p. 2954, 2970, ultima dată amendată de Articolul 1a al Legii din 31 iulie 2009, în *Federal Law Gazette I*, p. 2499, 2502, Secțiunea 9.

[26] Olanda, Intelligence and Security Services Act [Legea privind serviciile de informații și de securitate] 2002, Articolul 13.

[27] Argentina, National Intelligence Law [Legea privind informațiile naționale] 2001, Nr. 25520, Articolul 4.

3.3.2 Limite în privința dezvăluirii datelor cu caracter personal

Limitele legale în privința dezvăluirii de date cu caracter personal sunt, în general, de dorit, în special pentru a preveni scurgerea de informații din rațiuni politice partizane. Restricțiile de acest gen sunt deosebit de importante în statele de tranziție, acolo unde sarcina delicată de a clădi încrederea în neutralitatea instituțiilor de securitate poate fi puternic subminată de o conduită partizană. Multe țări stabilesc o răspundere penală pentru ofițerii de informații care dezvăluie informații din dosarele serviciului lor, inclusiv date cu caracter personal, fără a avea autoritatea legală sau în scopuri neautorizate (a se vedea Caseta 3).

Caseta 3: Interzicerea dezvăluirii abuzive a datelor cu caracter personal în România

Această prevedere din legislația română ilustrează modul în care datele cu caracter personal pot fi protejate împotriva dezvăluirii abuzive de către ofițerii de informații.

„Informațiile privind viaţa particulară, onoarea sau reputația persoanelor, cunoscute incidental în cadrul obținerii datelor necesare siguranței naționale, nu pot fi făcute publice. Divulgarea sau folosirea, în afara cadrului legal, de către salariații serviciilor de informații, a datelor prevăzute în alin. 1, constituie infracțiune și se pedepsește cu închisoare de la 2 la 7 ani.” [28]

3.3.3 Dezvăluirea publică a tipurilor de date stocate

În unele țări, legislația privind protecția datelor cere agențiilor de stat, precum serviciile de informații, să publice detalii despre tipurile de date cu caracter personal pe care le dețin, scopurile pentru care au fost culese, scopurile pentru care pot fi dezvăluite, descrieri ale bazelor de date în care sunt păstrate și condițiile și controalele aplicabile în cazul acestor baze de date. Publicarea unor asemenea informații contribuie la creşterea atât a transparenței, cât și a responsabilității. Persoanele care doresc să își exercite drepturile de acces la datele proprii și de rectificare a lor, în calitate de subiecți, pot afla din aceste informații care sunt agențiile de stat care dețin datele lor personale, precum și aria de cuprindere și motivele păstrării acestor date.

În principiu, este de dorit să se impună serviciilor de informații obligaţia de a dezvălui detalii despre datele cu caracter personal pe care le dețin deoarece atare demers ajută la consolidarea legitimității agențiilor și la eliminarea speculațiilor despre munca lor. O astfel de dezvăluire e benefică chiar atunci

[28] Legea privind siguranța națională a României, Articolul 21.

când există motive serioase, întemeiate pe rațiuni de securitate națională, ca o persoană să fie împiedicată să afle dacă datele cu caracter personal care o privesc sunt deținute de un serviciu de informații – de exemplu, acolo unde un răspuns la cererea de acces a subiectului, care „nici nu confirmă, nici nu neagă," ar fi justificat.

Caseta 4: Obligația de a dezvălui informații privind băncile de date conform legislației canadiene

Această prevedere din legislația canadiană ilustrează obligația generală de a face publice informații privind bazele de date ce conțin informații cu caracter personal:

> „Conducătorul unei instituții guvernamentale trebuie să dispună includerea în băncile de informații personale a tuturor informațiilor cu caracter personal, aflate sub controlul instituției guvernamentale, care (a) au fost utilizate, sunt în curs de utilizare sau sunt disponibile pentru utilizare în scop administrativ sau (b) sunt organizate sau urmează să fie consultate pe baza numelui unei persoane sau pe baza unui număr, a unui simbol sau a altui element particular de identificare, atribuit unei persoane."[29]

3.3.4 Accesul subiectului la datele sale cu caracter personal

Multe țări au adoptat legi referitoare la protecția datelor sau la viața privată, care recunosc dreptul subiecților unor date de a avea acces la datele lor personale, deținute de agențiile guvernamentale (a se vedea Caseta 5). Unele legi privind protecția datelor recunosc, în plus, dreptul subiecților de a rectifica asemenea informații, de a include în informațiile respective o declarație prin care contestă exactitatea lor sau de a determina distrugerea acestora. Din rațiuni de securitate națională, asemenea legi includ invariabil dispoziții speciale pentru datele deținute de serviciile de informații. Aceste dispoziții au o multitudine de forme.

În unele țări, serviciilor li se acordă o *scutire* de la prevederile legilor referitoare la protecția datelor, prevederi care, pur și simplu, nu se aplică în cazul informațiilor pe care le dețin. În astfel de situații, nu există vreun drept de acces al subiecților la propriile date. Această abordare are avantajul simplității, dar poate fi considerată drept excesiv de extinsă, deoarece excepțiile scutesc serviciile de orice obligație de a explica în ce mod restrângerea accesului la

[29] Canada, Privacy Act [Lege privind viața privată], R.S.C., 1985, Capitolul P-21, Secțiunea 10. O prezentare generală a băncilor de informații personale deținute de serviciile de securitate și de informații din Canada poate fi găsită la http://www.infosource.gc.ca/inst/csi/fed07-eng.asp.

anumite date este justificată de preocupările pentru securitatea națională. O asemenea abordare poate, totodată, să împiedice funcționarea unei supravegheri externe și a unor controale normale limitând, de exemplu, jurisdicția unui comisar pentru viața privată.

O variantă a acestei abordări este scutirea serviciilor de informații numai de prevederile legislației referitoare la libertatea informației. În asemenea cazuri, legile privind protecția datelor (inclusiv dreptul de acces al subiecţilor) continuă să se aplice, cel puțin în principiu, deși, în practică, sunt examinate de la caz la caz.

Caseta 5: Dreptul de acces la datele cu caracter personal deținute de serviciile de informații, conform legislației olandeze

Aceste dispoziții din legislația olandeză ilustrează un drept limitat de acces al subiectului la datele cu caracter personal deținute de serviciile de informații: [30]

„Articolul 47

1. Ministrul relevant va informa orice persoană, la cererea acesteia, cât mai curând posibil, dar cel mai târziu în termen de trei luni, dacă au fost prelucrate date personale care se referă la ea de către un serviciu sau în numele lui și, dacă da, care date anume."

„Articolul 48

1. Persoana care, potrivit Articolului 47, a consultat informațiile care o privesc, prelucrate de un serviciu sau în numele lui, poate prezenta o declarație scrisă în legătură cu acestea. Declarația va fi adăugată la informațiile respective."

„Articolul 53

1. O cerere precum cea menționată în Articolul 47 va fi în orice caz refuzată dacă:
   a. informațiile privind persoana care înaintează cererea au fost prelucrate în contextul oricărei investigații, cu excepția cazului în care:
      i. informațiile relevante au fost prelucrate cu mai mult de cinci ani înainte;
      ii. de atunci, nu au mai fost prelucrate informații noi privind persoana care face cererea, în legătură cu investigația pentru care au fost prelucrate informațiile în cauză, iar informațiile respective nu sunt relevante pentru nicio investigație în curs;
   b. niciun fel de informații nu au fost prelucrate cu privire la persoana care înaintează cererea."

Alte țări includ, în schimb, în legislația lor referitoare la protecția datelor, *excepții* bazate pe securitatea națională. Acestea sunt mai restrânse și mai

[30] Olanda, Intelligence and Security Services Act [Lege privind serviciile de informații și de securitate], 2002.

specifice decât scutirile, deoarece lasă în seama serviciului de informații sarcina de a justifica, de la caz la caz, motivul pentru care drepturile unei persoane, stipulate în legile privind protecția datelor, nu trebuie să se aplice.

Această legislație poate acorda persoanelor un drept *prima facie* de acces al subiectului, exercitat pur și simplu prin înaintarea unei solicitări către un organism de supraveghere, dar care este supus unor restricții ce au rolul de a proteja investigațiile în curs, precum și sursele și metodele.[31] (Toate restricțiile de acest gen trebuie să fie în conformitate cu legea de reglementare, proporționale cu amenințarea și supuse unei verificări independente [32]) Situată întru totul în afara drepturilor omului aflate în joc, o astfel de abordare poate oferi protecție împotriva unui management deficitar și a corupției.

În mod obișnuit, astfel de excepții permit unui serviciu să dea un răspuns prin care „nici nu confirmă, nici nu neagă," pentru a descuraja solicitările speculative și potențial periculoase, care urmăresc să evalueze amploarea informațiilor deținute de un serviciu.

În practică, aplicarea excepțiilor poate duce la refuzarea celor mai multe cereri. Astfel, rezultatul unei abordări prin exceptare pare să nu fie foarte diferit de rezultatul unei abordări prin scutire. Cu toate acestea, există o deosebire importantă: abordarea prin exceptare impune ca agenția să justifice refuzul de a dezvălui în raport cu prezumția legală în favoarea dezvăluirii, în vreme ce abordarea prin scutire nu impune justificarea. În plus, solicitarea unei excepții poate fi examinată de o autoritate independentă într-un mod în care solicitarea unei scutiri nu poate fi. Cercetarea empirică asupra modului în care operează în Canada „Legea privind accesul la informații" din 1982 și „Legea privind viața privată" din 1982 confirmă beneficiile ce rezultă din verificarea externă, realizată de un organism independent, a gestionării informațiilor de către ser-

---

31 A se vedea, de exemplu, Olanda, Intelligence and Security Services Act [Lege privind serviciile de informații și de securitate] 2002, Articolul 47; Suedia, Act on Supervision of Certain Crime-Fighting Activities [Lege privind supravegherea anumitor activități de combatere a criminalității], Articolul 3; Elveția, Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure [Lege federală care instituie măsuri pentru menținerea siguranței interne], Articolul 18 (1).

32 A se vedea, de exemplu, Olanda, Intelligence and Security Services Act [Lege privind serviciile de informații și de securitate], Articolele 53–56; Croația, Act on the Security Intelligence System [Lege privind sistemul informațiilor de securitate], Articolul 40 (2)(3).

viciile de informații – și, nu în ultimul rând, beneficiul unei sensibilizări sporite pe plan intern cu privire la preocupările legate de informații și viața privată.[33]

O altă variantă este desemnarea numai a anumitor bănci de date ca fiind „scutite," supunându-le astfel, în principiu, unor mecanisme de supraveghere diferite; în practică, serviciul de informații nu va mai avea obligația de a răspunde în detaliu cererilor individuale. Canada folosește acest model în completarea abordării prin exceptare.

Alternativ, legea de reglementare poate împuternici un ministru, cu condiția revizuirii, să elibereze un certificat de scutire cu caracter general (precum cel prevăzut în „Legea privind protecția datelor" din Marea Britanie[34]). Procedând astfel, va oferi în mare măsură serviciilor de informații siguranța că dosarele lor nu vor fi dezvăluite într-un mod care, de pildă, contravine angajamentelor asumate față de aliați și informatori. Pe de altă parte, asemenea certificate sunt, de regulă, excesiv de extinse, eliminând verificarea externă și beneficiile acesteia, inclusiv încrederea populației în corectitudinea serviciilor. Preocupă-

Caseta 6: Accesul la datele cu caracter personal deținute de serviciile de informații: bune practici identificate de Raportorul special al Națiunilor Unite

„Indivizii au posibilitatea de a solicita accesul la datele lor personale deținute de serviciile de informații. Ei își pot exercita acest drept prin înaintarea unei cereri către o autoritate competentă sau prin intermediul unei instituții independente de protecție a datelor sau de supraveghere. Indivizii au dreptul de a rectifica inexactitățile din datele lor personale. Orice excepții de la aceste reguli generale sunt prevăzute prin lege și strict limitate, proporționale și necesare pentru îndeplinirea mandatului serviciului de informații. Acesta trebuie să justifice în fața unei instituții independente de supraveghere orice decizie prin care refuză dezvăluirea informațiilor cu caracter personal."[35]

---

[33] Ian Leigh, „Legal Access to Security Files: the Canadian Experience" [„Accesul legal la dosarele de securitate: experiența canadiană"], în *Intelligence and National Security* 12, no. 2 (1997), p. 126. Pentru acest studiu, au fost luate interviuri unor oficiali din Serviciul Canadian pentru Informații de Securitate, comisarilor pentru informații și viața privată şi staffului acestora, utilizatorilor legislației, judecătorilor din instanțele federale și altor experți.

[34] Marea Britanie, Data Protection Act [Lege privind protecția datelor] 1998, Secțiunea 28.

[35] Consiliul Națiunilor Unite pentru Drepturile Omului *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, p. 23 (Practica 26).

rilor legitime în privința securității informațiilor li se răspunde mai bine prin exceptări specifice decât prin scutiri cu caracter general. Mai mult, în afară de accesul subiecților la date și posibilitatea rectificării lor, principiile de protecţie a datelor, referitoare la calitatea și securitatea acestora, au, de asemenea, o importanță evidentă pentru serviciile de informații și, în consecință, oferă încă un motiv pentru a nu scuti serviciile de jurisdicția legilor de protecție a datelor.

3.3.5 Notificarea faptului că au fost culese date cu caracter personal

Unele țări (precum Olanda[36] și Germania[37]) impun ca subiecții culegerii (îndeosebi prin urmărire) de date cu caracter personal să fie înștiințați ex post facto, iar datele strânse despre ei să se încadreze în anumite limite (a se vedea Caseta 7). În teorie, această practică oferă posibilitatea unei contestări retroactive și permite o verificare a deciziei serviciilor de informații de a alcătui un dosar referitor la subiectul vizat. Totuși, restricțiile în privința dreptului de notificare, având ca scop protejarea operațiunilor în desfășurare și a identității surselor, pot face ca acest drept să fie iluzoriu în multe situații. Din acest motiv, practica sus-menționată este actualmente în curs de revizuire în Olanda.[38]

Alternativ, acolo unde nu există dreptul de notificare sau rectificare, riscurile asociate utilizării datelor cu caracter personal de către serviciile de informații vor fi, fără îndoială, exacerbate, iar nevoia de a se efectua alte controale va fi, în mod corespunzător, mai mare.

3.3.6 Verificarea, corectarea și ștergerea datelor cu caracter personal

O altă modalitate de aplicare a principiilor de protejare a datelor poate fi pusă în practică atunci când serviciilor de informații li se impune să verifice periodic dacă dosarele pe care le deţin, conținând date cu caracter personal, sunt exacte, actualizate și relevante pentru mandatul lor.[39] În unele țări, această

---

[36] În conformitate cu Articolul 34 din *The Intelligence and Security Services Act* [*Legea privind serviciile de informații și de securitate*], 2002, începând cu cinci ani după ce un serviciu de informații și-a exercitat o putere specială de investigare (și, ulterior, anual) „ministrul relevant va examina dacă un raport privind evenimentul poate fi prezentat persoanei în privința căreia a fost exercitată una din aceste puteri speciale. Dacă e posibil, prezentarea raportului va fi făcută în cel mai scurt timp."

[37] Germania, Federal Act on Protection of the Constitution [Legea federală privind protejarea Constituției], Secțiunea 9.3.

[38] Olanda, Comisia de Verificare a Serviciilor de Informații și de Securitate (CTIVD), *Annual Report 2010*–2011 [*Raportul anual 2010–2011*], Capitolul 4.

[39] De exemplu, a se vedea Germania, Federal Act on Protection of the Constitution [Legea federală privind protejarea Constituției], Secțiunea 14.2; Germania, G10 Act [Legea G10], Secțiunile 4.1 și 5; Elveția, Loi fédérale instituant des mesures visant au

Caseta 7: Obligația de a notifica subiecții datelor conform legislației germane

Aceste dispoziții din legislația germană ilustrează principiul notificării:

„Subiectul datelor va fi informat în privința măsurilor restrictive adoptate în conformitate cu Secțiunea 3, după ce acestea au fost suspendate. O asemenea notificare va fi blocată atâta vreme cât nu se exclude faptul că înștiințarea subiectului căruia îi aparțin datele ar putea să prejudicieze scopul restricționării sau atâta vreme cât se preconizează că notificarea ar aduce orice fel de dezavantaje generale la adresa intereselor Federației ori ale unui stat federal. Acolo unde o astfel de notificare continuă să fie blocată (potrivit celei de-a doua fraze) timp de 12 luni după suspendarea măsurii, continuarea amânării necesită aprobarea de către Comisia G10. Comisia G10 va stabili durata amânării.” [40]

„În ceea ce privește culegerea de date în conformitate cu subsecțiunile 2 și 1, ale cărei natură și importanță sunt echivalente cu o restrângere a caracterului privat al scrisorilor, poștei și telecomunicațiilor, constând îndeosebi în ascultarea și înregistrarea conversațiilor private cu ajutorul unor mijloace tehnice clandestine,

1. subiectul datelor va fi informat asupra măsurii după suspendarea acesteia, de îndată ce se exclude faptul că scopul măsurii e prejudiciat, iar
2. Comisia specială de control parlamentar va fi notificată în acest sens.” [41]

obligație e asociată cu obligațiile suplimentare de a corecta sau distruge informațiile care sunt incorecte [42] sau care nu mai sunt relevante.[43]

Dacă numai în acest mod rapoartele lor se pot baza pe informații exacte, serviciile de informații trebuie să stabilească proceduri pentru verificarea și corectarea datelor cu caracter personal ca să se asigure că ele sunt la zi și complete (în măsura în care acest lucru este relevant pentru activitățile legale ale servi-

maintien de la sûreté intérieure [Legea federală care instituie măsuri pentru menținerea siguranței interne], Articolul 15 (1) (5).

[40] Germania, Act Restricting the Privacy of Correspondence, Posts, and Telecommunications (G10 Act) [Legea privind restricționarea caracterului privat al corespondenței, poștei și telecomunicațiilor („Legea G10”)] (26 iunie 2001), în *Federal Law Gazette I*, p. 1254, revizuit 2298, ultima dată amendată de Articolul 1 din Legea din 31 iulie 2009, în *Federal Law Gazette I*, p. 2499, Secțiunea 12.1.

[41] Germania, Federal Act on Protection of the Constitution [Legea federală privind protejarea Constituției], Secțiunea 9.3.

[42] Olanda, Intelligence and Security Services Act [Legea privind serviciile de informații și de securitate], 2002, Articolul 43; Croația, Act on the Security Intelligence System [Lege privind sistemul informațiilor de securitate], Articolul 41(1).

[43] Germania, Federal Act on Protection of the Constitution [Legea federală privind protejarea Constituției], Secțiunea 12.2.

ciilor). Datele depășite pot fi înșelătoare și, prin urmare, mai periculoase chiar decât necunoașterea lor. În plus, din punctul de vedere al subiectului datelor, este mult mai puțin probabil ca informațiile cu caracter personal care sunt corecte și la zi să ducă la o nedreptate, așa cum ar fi refuzul eliberării certificatului de securitate sau o decizie defavorabilă imigrării.

Caseta 8: Evaluări regulate ale datelor deținute de serviciile de informații: bune practici identificate de Raportorul special al Națiunilor Unite

„Serviciile de informații efectuează evaluări regulate cu privire la relevanța și exactitatea datelor personale pe care le dețin. Lor li se impune prin lege să șteargă sau să actualizeze orice informații apreciate ca inexacte sau ca nemaifiind relevante pentru propriul mandat, pentru activitatea instituțiilor de supraveghere sau pentru eventuale acțiuni în justiție.”[44]

Datorită naturii preventive și de anticipare a evaluării amenințărilor, efectuată de serviciile de informații, unele persoane pot atrage în mod legitim atenția serviciilor înainte de culegerea unor informații suplimentare, care stabilesc că nu mai sunt ținte potrivite pentru o culegere ulterioară de date. Se poate descoperi, de exemplu, că un subiect e asociat cu o țintă legitimă, însă el însuși / ea însăși nu este un conspirator; sau subiectul poate avea pur și simplu un nume similar cu cel al unei ținte legitime. A impune unui serviciu de informații să-și închidă dosarul privind subiectul în cauză poate preveni un posibil abuz.

În mod asemănător, informațiile tangențiale referitoare la unele persoane, culese în cursul unei operațiuni care s-a desfășurat, trebuie să fie șterse. Legea germană ce reglementează activitățile Oficiului Federal pentru Protecția Constituției conține mai multe dispoziții relevante pentru această preocupare. Ea prevede, de pildă, că strângerea informațiilor trebuie să înceteze „de îndată ce scopul său a fost atins sau dacă există indicații că scopul nu poate fi atins deloc sau nu poate fi atins prin utilizarea informaţiilor respective.”[45] Legea impune totodată obligațiile de verificare (la fiecare cinci ani) a datelor culese anterior, de corectare a datelor inexacte (prin indicarea în dosarele aferente a datelor inexacte sau contestate [46]) și de ștergere a datelor care nu mai sunt

[44] Consiliul Națiunilor Unite pentru Drepturile Omului *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, p. 22 (Practica 24).

[45] Germania, Federal Act on Protection of the Constitution [Legea federală privind protejarea Constituției], Secțiunea 9.1.

[46] Ibid., Secțiunea 13.

Caseta 9: Obligațiile de verificare, corectare și ștergere a datelor cu caracter personal în conformitate cu legislația germană

Aceste prevederi din legislația germană ilustrează principiile de verificare, modificare și ștergere:

(1) Datele personale incorecte, stocate în dosare, trebuie corectate de Oficiul Federal pentru Protecția Constituției.

(2) Datele personale stocate în dosare trebuie să fie șterse de Oficiul Federal pentru Protecția Constituției dacă stocarea lor a fost neadmisibilă sau dacă nu mai este necesară cunoașterea lor pentru îndeplinirea sarcinilor sale. Datele nu vor fi șterse dacă există motive pentru a considera că ștergerea ar afecta interesele legitime ale subiecților cărora le aparțin. Într-un astfel de caz, datele vor fi blocate și vor fi transferate numai cu consimțământul subiectului în cauză.

(3) Atunci când examinează cazuri particulare, Oficiul Federal pentru Protecția Constituției va verifica la termene specificate, cel mai târziu după cinci ani, dacă datele personale trebuie să fie corectate sau șterse.[47]

necesare (a se vedea Caseta 9). În afara protejării subiecților cărora le aparțin datele, aceste obligații ajută activitatea de supraveghere.

4. ROLUL ORGANISMELOR DE SUPRAVEGHERE

Secțiunea de față prezintă căile prin care organismele de supraveghere pot monitoriza utilizarea de către serviciile de informaţii a datelor cu caracter personal, pentru a se asigura că aceste date nu sunt folosite incorect. Cu toate că se axează, în principal, pe supravegherea externă, importanța mecanismelor interne nu trebuie neglijată. Acestea includ proceduri specifice pentru a determina momentul în care dosarele trebuie deschise ori închise, care membri ai personalului trebuie să aibă acces la ele, momentul în care conținutul dosarelor trebuie verificat și modul în care vor fi păstrate în siguranță.

Pe de altă parte, o supraveghere externă eficace depinde de existența unor organisme independente care au competențe legale și resurse adecvate pentru a-și duce la îndeplinire mandatul (a se vedea Tabelul 2). Raportorul special al Națiunilor Unite a subliniat necesitatea unei instituții independente care „are acces la toate dosarele deținute de serviciile de informații și are puterea de dispune comunicarea informațiilor către persoanele în cauză, precum și distrugerea dosarelor sau a informațiilor personale.”[48] *Carta drepturilor fun-*

[47] Ibid., Secțiunea 12.

[48] Consiliul Națiunilor Unite pentru Drepturile Omului *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, p. 22 (Practica 25).

damentale a Uniunii Europene prevede că respectarea regulilor de protecție a datelor „se supune controlului unei autorități independente."[49] La nivel național, legislația suedeză garantează autonomia și resursele Comisiei suedeze pentru Protejarea Securității și Integrității,[50] în vreme ce legislația ungară impune serviciilor de informații obligația specifică de a coopera cu organismele independente de supraveghere în ceea ce privește utilizarea datelor personale.[51]

TABELUL 2: CARACTERISTICILE ORGANISMELOR EXTERNE INDEPENDENTE DE SUPRAVEGHERE				
Instituția	Independența	Domeniul de activitate	Metode	Rezultate
Instituția de tip ombudsman	Autonomă	Reclamații individuale	Investigare	Recomandări
Comisarul pentru protecția datelor	Autonom	Respectarea legilor de protecție a datelor	Investigare, verificare prin sondaj	Raport, directive
Tribunalul	Autonom	Reclamații individuale	Proces în instanţă	Decizie obligatorie
Comisia parlamentară	Partizană	Trimitere spre rezolvare, raportare din proprie inițiativă	Audieri parlamentare	Raport

În statele aflate în tranziție și după conflict, serviciile recent democratizate iau adeseori în custodie arhive voluminoase cu dosare de securitate, ce conțin informații culese în regimul anterior. Gestionarea unor asemenea dosare poate pune probleme neobișnuite, îndeosebi atunci când (din rațiuni democratice temeinice) sectorul de securitate și informații al țării a fost drastic redus ca dimensiuni. În asemenea situații, organismele independente de supraveghere

49 Uniunea Europeană, Charter of Fundamental Rights of the European Union [Carta drepturilor fundamentale a Uniunii Europene], Articolul 8.3.

50 Suedia, Ordinance containing instructions for the Swedish Commission on Security and Integrity Protection [Ordonanță conţinând instrucțiuni pentru Comisia suedeză pentru Protejarea Securității și Integrității], Secțiunile 4–8 (cu privire la conducere și luarea deciziilor) și 12–13 (cu privire la resurse și suport).

51 Ungaria, Act on the National Security Services [Lege privind serviciile de securitate națională], Secțiunea 52.

pot juca un rol util prin efectuarea unui control al practicilor de gestionare a dosarelor, folosind în acest scop diverse mijloace.

În general, funcțiile organismelor independente de supraveghere, ce se referă la datele cu caracter personal, sunt reglementate, în parte, prin norme stabilite de legislația în materia drepturilor omului. În privința recursului *post hoc*, de exemplu, Articolul 13 al ECHR stabilește că „Orice persoană, ale cărei drepturi şi libertăţi …. au fost încălcate, are dreptul să se adreseze efectiv unei instanţe naţionale." În decizia sa în cazul *Segerstedt-Wiberg versus Suedia* (2006), CEDO a considerat că, deși condiția din Articolul 13 este, în general, subsidiară condițiilor din Articolul 8 privind „conformitatea cu legea" și „necesitatea într-o societate democratică," absența din legislația națională a unei prevederi privind recursul poate duce la încălcarea Convenției. În alte situații, Curtea a reținut că procedura recursului, cerută în Articolul 13, trebuie să fie efectivă în practică, precum și în lege, chiar în contextul securității naționale.[52]

În cazul *Asociația pentru Integrare Europeană și Drepturile Omului versus Bulgaria*, privind o situație de interceptare a comunicațiilor, în care se pretindea încălcarea atât a Articolului 8, cât și a Articolului 13, Curtea a făcut trimitere, în susținere, la mai multe exemple de recursuri independente care răspund cerințelor Convenției. Acestea au inclus: dreptul de a reclama în fața unui organism specializat de supraveghere (Comisia G10) și a Curții Constituționale în Germania; dreptul de apel în fața Consiliului de Stat în Luxemburg; dreptul de recurs în fața unui tribunal special în Marea Britanie; și dreptul de a reclama în fața unui organism specializat de supraveghere în Norvegia.[53] (Pentru o discuție detaliată privind gestionarea reclamațiilor, a se vedea Forcese – Instrumentul 9.)

În ceea ce privește utilizarea datelor cu caracter personal de către serviciile de informații, aspectele principale ale supravegherii le reflectă pe cele din normele legale, și anume culegerea datelor, stocarea datelor, accesul subiecților, notificarea, verificarea, rectificarea și ștergerea. Deoarece aceste aspecte au o sferă largă de cuprindere, jurisdicția organismelor de supraveghere trebuie să fie la fel de mare. De exemplu, autoritatea Comisiei germane G10 se extinde asupra „întregii arii a culegerii, prelucrării și utilizării datelor personale obținute în conformitate cu această lege de către serviciile de informații ale

[52] *Al-Nashif v. Bulgaria* [*Al-Nashif versus Bulgaria*], Nr. 50963/99, CEDO, 2002, Paragraful 136.

[53] *Association for European Integration and Human Rights v. Bulgaria* [*Asociația pentru Integrare Europeană și Drepturile Omului versus Bulgaria*], Nr. 62540/00, CEDO, Paragraful 100.

Caseta 10: Comisia de Control al Serviciilor de Informații ale Poliției și Armatei (Comisia Wamberg) din Danemarca

Sarcina principală a Comisiei Wamberg este de a supraveghea înregistrarea și diseminarea datelor cu caracter personal de către Serviciul danez de Securitate și Informații (PET). Atunci când o persoană sau o organizație devine subiectul unei investigații pentru obținerea de informații, PET poate dori să deschidă un dosar privind acea persoană sau organizație. Asemenea dosare sunt supuse verificării de către Comisia Wamberg, care trebuie să aprobe înregistrarea de noi dosare referitoare la cetățeni danezi și cetățeni străini rezidenți în Danemarca.

Comisia este compusă dintr-un președinte și alți trei membri. Toți sunt numiți în temeiul încrederii generale și al respectului de care se bucură. Totodată, fiecare dintre ei trebuie considerat a fi apolitic.

Comisia se întrunește de șase până la zece ori pe an în birourile PET pentru a examina cazurile și a decide dacă criteriile pentru înregistrarea lor au fost îndeplinite. În același timp, comisia ia mostre aleatorii din dosarele vechi pentru a stabili dacă termenele pentru ștergerea lor sunt respectate. Totodată, comisia discută regulat cu Ministerul Justiției despre principiile de înregistrare.

Federației, inclusiv asupra deciziei de notificare a subiecților cărora le aparțin datele.”[54]

Supravegherea de acest gen este necesară pentru a asigura respectarea de către servicii a normelor referitoare la datele cu caracter personal menționate mai sus. Ținând seama de natura secretă a muncii de informaţii, există o probabilitate mai mare ca o astfel de supraveghere să fie eficace și să determine respect din partea opiniei publice dacă este continuă (sau cel puțin periodică), decât dacă are loc ca simplă reacție la reclamațiile sau alegațiile de abuz făcute în mod public. Drept urmare, mai multe țări au adoptat prevederi privind examinarea pe baze permanente în cadrul mandatelor atribuite organismelor independente, responsabile cu supravegherea serviciilor de informații. De exemplu, în Norvegia, Comisia parlamentară de supraveghere a serviciilor de informații (un organism specializat de supraveghere) are obligația legală de a efectua anual șase inspecții la Serviciul de Securitate al Poliției norvegiene. Aceste inspecții trebuie să cuprindă cel puțin 10 verificări aleatorii în arhivă și,

---

[54] Hans De With și Erhard Kathmann, „Parliamentary and Specialised Oversight of Security and Intelligence Agencies in Germany” [„Supravegherea parlamentară și specializată a agențiilor de securitate și de informații în Germania”], în *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, Aidan Wills și Mathias Vermeulen (Bruxelles: Parlamentul European, 2011), Anexa A, p. 220.

cel puțin de două ori pe an, câte o verificare a tuturor cazurilor de urmărire aflate în desfășurare.[55] Comisia de Control al Serviciilor de Informații ale Poliției și Armatei din Danemarca (Comisia Wamberg, denumită astfel după numele primului său președinte, A.M. Wamberg) îndeplinește un rol similar (a se vedea Caseta 10).

Caseta 11: Comisia pentru Protejarea Securității și Integrității din Suedia

Aceste prevederi din legislația suedeză descriu responsabilitățile Comisiei pentru Protejarea Securității și Integrității (un organism specializat de supraveghere):

(1) Comisia pentru Protejarea Securității și Integrității (Comisia) va supraveghea utilizarea de către agențiile de combatere a criminalității a urmăririi secrete și schimbării de identitate, precum și a activităților asociate.
Comisia va supraveghea și prelucrarea datelor de către Serviciul de Securitate suedez, în conformitate cu „Legea privind protecția datelor deținute de poliție”, îndeosebi potrivit Secțiunii 5 a acestei legi.
Supravegherea va avea ca scop, în mod special, să se asigure că activitățile menționate în primul și al doilea paragraf sunt efectuate în concordanță cu legile și celelalte reglementări.

(2) Comisia își va exercita supravegherea prin intermediul inspecțiilor și al altor investigații.
Comisia poate să facă declarații referitoare la circumstanțe identificate și să-și exprime opinia cu privire la necesitatea de a aduce modificări activităților în cauză și se va strădui să se asigure că orice deficiențe ale legilor și celorlalte reglementări sunt remediate.

(3) La cererea unei persoane, comisia este obligată să verifice dacă el sau ea a fost subiectul unei urmăriri secrete sau al prelucrării datelor sale personale, așa cum sunt definite în Secțiunea 1 și dacă utilizarea urmăririi secrete și activitățile asociate ori prelucrarea datelor sale personale au fost în concordanță cu legile și cu celelalte reglementări. Comisia va notifica persoana respectivă că s-a efectuat verificarea.[56]

[55] Norvegia, Instructions for Monitoring of Intelligence, Surveillance and Security Services [Instrucțiuni pentru monitorizarea serviciilor de informații, supraveghere și securitate], Secțiunile 11.1 (c) și 11.2 (d).

[56] Suedia, Act on Supervision of Certain Crime-Fighting Activities [„Lege privind supravegherea anumitor activități de combatere a criminalității”] (2007); a se vedea și Suedia, Ordinance containing instructions for the Swedish Commission on Security and Integrity Protection [Ordonanță conţinând instrucțiuni pentru Comisia suedeză pentru Protejarea Securității și Integrității] (2007), Secțiunea 2 (disponibil la http://www.sakint.se/dokument/english/ordinance_instruction_scsip.pdf).

Într-o serie de țări, o persoană care reclamă modul în care un serviciu de informații a gestionat datele sale personale poate fi audiată de un organism independent, ce are competența de a inspecta dosarele serviciului și de a stabili dacă datele respective au fost folosite incorect (a se vedea Forcese – Instrumentul 9). De pildă, în conformitate cu legislația suedeză, Comisia pentru Protejarea Securității și Integrității are autoritatea, atunci când răspunde unei reclamații, de a verifica legalitatea activităților desfășurate de serviciul de securitate în ceea ce privește utilizarea datelor cu caracter personal (a se vedea Caseta 11). Comisia are și autoritatea de a verifica transmiterea datelor personale din diferite registre de poliție și securitate, cu scopul de a se asigura că difuzarea în cauză respectă legea statutară şi constituţională suedeză, inclusiv normele privind drepturile omului și principiul proporționalității.[57]

5. RECOMANDĂRI

Secțiunea de față recomandă principiile pe care parlamentarii, în mod special, le pot urma în stabilirea unui cadru legal adecvat pentru utilizarea de către serviciile de informaţii a datelor cu caracter personal într-o manieră compatibilă cu obligațiile în materia drepturilor omului.

- Mandatul dat de legislativ fiecărui serviciu de informații trebuie să precizeze scopurile pentru care datele cu caracter personal pot fi culese în mod legal, iar dosarele – deschise în mod legal.
- Legea care reglementează serviciile de informații trebuie să dispună controale efective asupra modului în care datele cu caracter personal sunt folosite și a duratei pe care pot fi păstrate. Aceste controale trebuie să respecte principiile internațional acceptate cu privire la protecția datelor. O astfel de lege trebuie să impună și verificări efectuate de un personal independent (adică de verificatori din afara comunității de informații) pentru a asigura efectuarea unor controale reale.
- Legea care reglementează serviciile de informații nu trebuie să le scutească pe acestea de prevederile legilor interne referitoare la viața privată și protecția datelor. În schimb, serviciilor trebuie să li se permită, atunci când este relevant pentru mandatele lor, să beneficieze de excepțiile de la reglementările privind dezvăluirea datelor în temeiul unui concept restrâns de securitate națională.

57 Iain Cameron, „Parliamentary and Specialised Oversight of Security and Intelligence Activities in Sweden” [„Supravegherea parlamentară și specializată a activităților de securitate și de informații în Suedia”], în *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, Aidan Wills și Mathias Vermeulen (Bruxelles: Parlamentul European 2011), Anexa A, pp. 279–81.

- Aplicarea corectă, sau nu, a acestor excepții trebuie determinată de un organism independent de supraveghere, care dispune de un acces corespunzător la datele relevante din dosarele serviciului.
- Persoanele care reclamă încălcarea vieții lor private prin stocarea, utilizarea sau dezvăluirea datelor lor personale de către un serviciu de informații trebuie să aibă dreptul la un recurs efectiv în fața unui organism independent.
- Deciziile serviciilor de informații de a stoca date cu caracter personal trebuie verificate de un organism independent de supraveghere, tot așa cum trebuie să fie și cererile subiecților de acces, precum și deciziile de păstrare, transferare și ștergere ale respectivelor date.

INSTRUMENTUL 7

Supravegherea schimbului de informații

Kent Roach



7

Supravegherea schimbului de informații

Kent Roach

1. INTRODUCERE

Acest instrument examinează provocările generate de dezvoltarea schimburilor de informații, cu care se confruntă activitatea de supraveghere a serviciilor de informații și a altor structuri guvernamentale care culeg, analizează și distribuie informații privind securitatea națională.[1] Termenul de *schimb de informații* se referă aici la informațiile care sunt schimbate între serviciile de informații și agențiile partenere, fie ele străine sau naționale. Deși acest instrument se axează în principal pe organismele de supraveghere, el analizează și implicațiile asupra drepturilor omului și a vieții private, pe care le are extinderea schimburilor de informații – ceea ce poate prezenta interes şi pentru alte entități, așa cum sunt ramurile judiciară și executivă ale guvernării, mass-media și societatea civilă.

Serviciile de informații au avut întotdeauna sarcina de a comunica informațiile pe care le culeg. Cu toate acestea, de la atacurile teroriste din 11 septembrie 2001, s-a pus un accent mult mai mare pe schimbul de informații pe plan internațional, între serviciile de informații, precum și între serviciile de informații și alte entități. Din motive evidente, creșterea volumului de informații transmise și a numărului de servicii implicate a făcut ca și problemele asociate acestei creșteri să fie mai mari. Informațiile transmise pot fi inexacte, ducând la alocarea greșită de către primitor a resurselor limitate de care dispune. În plus, ele pot fi folosite într-un mod inadecvat de serviciul care le

[1] Termenul de *serviciu de informații* este folosit aici cu sensul de organizație guvernamentală, ale cărei sarcini principale sunt culegerea și analizarea informațiilor privind securitatea națională și transmiterea lor către decidenţi. Această definiție a fost preluată din lucrarea lui Aidan Wills, *Guidebook: Understanding Intelligence Oversight,* Toolkit – Legislating for the Security Sector [*Ghid pentru înțelegerea activității de supraveghere a serviciilor de informații*, Set de instrumente – Legiferarea pentru sectorul de securitate] (Geneva, DCAF, 2010), p. 10.

primește. În unele situații extreme, se poate chiar ca serviciile să devină complice la tortură și la alte abuzuri împotriva drepturilor omului, comise fie de furnizorul, fie de primitorul de informații.

Practicile incorecte în comunicarea informațiilor pot dăuna grav reputației statului furnizor, așa cum s-a dovedit recent în cazul schimburilor de informații între serviciile de informații libiene, americane și britanice.[2] Și mai semnificative încă sunt prejudiciile grave pe care le poate avea schimbul defectuos de informații asupra reputației unor persoane. Asemenea consecințe regretabile fac ca supravegherea efectivă a practicilor asociate schimbului de informații să fie deosebit de importantă, chiar dacă informațiile furnizate sunt, frecvent, strict clasificate. Supravegherea acestor practici este deosebit de importantă, deoarece asemenea activități se desfășoară în mod normal în secret și, deci, nu sunt verificate cu ușurință în instanțe sau de către mass-media. Este posibil ca cei care pot fi afectați de schimbul de informații să nici nu știe că au fost afectați și nici să nu poată depune o plângere. În general, organismele de supraveghere au nevoie de acces la informațiile care au fost transmise. Altminteri, ele nu vor fi capabile să verifice în mod real practicile în materie ale serviciilor de informații pe care le supraveghează. Totuși, intensificarea recentă a schimbului de informații, precum și caracterul secret al informațiilor respective atrag provocări pentru organismele de supraveghere, care cu greu ar putea fi supraestimate.

Acest instrument începe cu o scurtă examinare a schimburilor de informații în lumea de după evenimentele din 11 septembrie 2001. Sunt studiate, în principal, provocările cu care se confruntă organismele de supraveghere în ceea ce priveşte comunicarea de informații în plan extern și, apoi, în cel intern, cu referire atât la primirea, cât și la diseminarea informațiilor. Capitolul se încheie cu recomandări specifice pentru a ameliora supravegherea comunicării de informații. Recomandările se referă nu numai la aspecte care vizează politicile, organizarea şi conducerea supravegherii, ci și la cadrul legal care poate reglementa de o manieră mai eficace schimbul de informații.

2 BBC News, „Libya: Gaddafi regime's US-UK spy links revealed" [Știrile BBC, „Libia: Dezvăluirea legăturilor de spionaj dintre serviciile de informații din SUA și Marea Britanie și regimul Gaddafi"], 3 septembrie 2011 (disponibil la: www.bbc.co.uk/news/world-africa-14774533).

2. SCHIMBUL DE INFORMAȚII

2.1 NEVOIA DE A FACE SCHIMB DE INFORMAȚII

Este evident că serviciile de informații, atât externe, cât și interne, au nevoie să facă schimb de informații pentru a răspunde în mod eficace amenințărilor complexe la adresa securității, cu care se confruntă. Oricum, în mediul transnațional actual, a fost adesea subliniată nevoia de dezvoltare a schimburilor de informații. De exemplu, în Rezoluția 1373 (din 28 septembrie 2001), Consiliul de Securitate al Națiunilor Unite a cerut în mod expres intensificarea schimburilor de informații între statele membre. În Europa, instituții precum Europol, Clubul de la Berna, Statul-Major al Uniunii Europene și Centrul de Situații al Uniunii Europene au pledat pentru creșterea comunicării de informații.[3] Drept rezultat, țări cu tradiții foarte diferite, care, altfel, poate n-ar fi fost dornice să se angajeze împreună în operațiuni comune de securitate, sunt totuși pregătite, în prezent, să facă schimb de informații privind nu doar combaterea terorismului, ci și operațiuni militare și de menținere a păcii, inspecții ale armamentului și urmărirea în justiție a crimelor de război.

Nivelul pe care l-a atins în prezent schimbul de informații dintre serviciile de informații este dificil de estimat, deoarece informațiile sunt secrete, tot așa cum sunt și înțelegerile pe baza cărora se face schimbul de informații. Cu toate acestea, datele disponibile oferă o oarecare imagine a dimensiunilor atinse. De pildă, serviciile interne de informații din Canada și Australia fac, fiecare, schimburi de informații cu circa 250 de agenții externe. Agenția Centrală de Informații din SUA (CIA) are stabilite relații cu peste 400 de agenții din întreaga lume.[4] Aceste schimburi se produc atât formal, cât și informal.

Din cauza naturii complexe a amenințărilor actuale, țările care respectă drepturile omului se pot simți uneori constrânse să facă schimb de informații cu națiuni care au performanțe scăzute în ceea ce privește respectarea drepturilor omului. Un serviciu poate considera că trebuie să avertizeze o țară în privința unei persoane suspectate de terorism, care a intrat sau plănuiește să intre în țara respectivă, chiar dacă țara care primește informațiile poate să aibă antecedente de abuzuri împotriva drepturilor omului. Totodată, e de la

3 James Walsh, „Intelligence-Sharing in the European Union: Institutions Are Not Enough” [„Schimbul de informații în Uniunea Europeană: instituțiile nu sunt suficiente”], în *Journal of Common Market Studies* 44, no. 3 (septembrie 2006), pp. 625–643.

4 Elizabeth Sepper, „Democracy, Human Rights and Intelligence Sharing” [„Democrația, drepturile omului și schimbul de informații”], în *Texas International Law Journal* 46 (2010), p. 155.

sine înțeles că furnizorii de informații se așteaptă la un anumit grad de reciprocitate din partea celor care au primit informațiile.

În deceniul de după evenimentele din 11 septembrie 2001, multe guverne naționale au făcut eforturi pentru a elimina barierele legale și organizaționale în schimbul de informații între agențiile interne cu responsabilități în materie de securitate și intelligence. Ceea ce este valabil, în special, în SUA, unde o comisie guvernamentală a stabilit că barierele dintre agențiile de informații și de securitate s-ar putea să fi împiedicat identificarea unora dintre teroriștii de la 11 septembrie 2001.[5] Drept rezultat, noul zel în favoarea schimbului de informații s-a extins mult dincolo de combaterea terorismului, vizând o gamă largă de responsabilități legate de aplicarea legii, inclusiv în domenii precum siguranța frontierelor, imigrația, contrabanda și spionajul.

2.2 PROBLEME GENERATE DE SCHIMBUL DE INFORMAȚII

Deși există un larg consens în privința faptului că schimbul de informații este necesar pentru întărirea securității, recenta expansiune a acestuia a generat o serie de probleme potențiale, care impun o gestionare și o supraveghere vigilente. De exemplu, agențiile de aplicare a legii sunt acum mai predispuse să acţioneze pe baza unor informații nesigure pe care le-au primit, așa că, în prezent, există un risc mai mare ca informațiile furnizate de serviciile de informații să fie dezvăluite în cadrul unor acțiuni ulterioare în justiție. La rândul lor, indivizii sunt expuși într-o mai mare măsură riscului de a le fi încălcate drepturile, îndeosebi dreptul la viață privată. Indivizii vor avea rareori ocazia să conteste exactitatea informațiilor furnizate, fiindcă, cel mai adesea, nu vor ști că au fost comunicate informații despre ei și nu vor avea acces la respectivele informații.

În multe țări, serviciile de informații au fost, prin tradiție, reticente să comunice informații secrete poliției și altor agenții de aplicare a legii. O comisie de anchetă din Canada a ajuns la concluzia că o asemenea reticență a contribuit la reușita atentatului cu bombă din 1985 asupra avionului companiei Air India, precum și la o serie de deficiențe în investigațiile care au avut loc după explozie.[6] Serviciile de informații au tendința de a păstra informațiile, fiindcă se tem că, odată comunicate, vor fi divulgate până la urmă, ceea ce ar putea însemna expunerea unor surse și metode importante și ar pune în pericol capacitatea serviciului de a culege informații în viitor. În plus, dacă informațiile au fost

5 Ernest R. May (ed.), *The 9 /11 Commission Report* [*Raportul Comisiei 11 septembrie*] (New York: St. Martins Press, 2007), Secțiunea 3.2.

6 Comisia de anchetă pentru investigarea exploziei cu bombă în cursa 182 a companiei Air India, *Air India Flight 182: A Canadian Tragedy* [*Zborul 182 al companiei Air India: o tragedie canadiană*] (2010).

obținute într-o manieră considerată neadmisibilă în cadrul unei acțiuni judiciare, transmiterea lor către agențiile de aplicare a legii poate deveni și mai problematică. Forțele de poliție, deși mai dispuse, probabil, decât serviciile de informații, să facă schimb de informații, sunt, la rândul lor, preocupate de faptul că furnizarea informațiilor pe care le dețin va perturba propria lor capacitate de a investiga și urmări în justiție cazurile care constituie amenințări la adresa securității.

Organismele însărcinate cu supravegherea serviciilor de informații se confruntă cu unele din cele mai serioase provocări. Ele trebuie să țină pasul cu volumul imens de informații care fac obiectul schimburilor la ora actuală, un volum atât de mare, încât aceste organisme se văd frecvent obligate să se bazeze pe controale care vizează doar un segment al informațiilor. Cele mai multe organisme de supraveghere întâmpină, de asemenea, dificultăți în obținerea accesului și urmărirea traseului urmat de informațiile secrete care au fost transmise. De pildă, e posibil ca un organism de supraveghere în a cărui jurisdicție intră poliția să nu aibă autoritatea de a afla cum au fost culese informațiile obținute de poliție de la un serviciu de informații. Ceea ce este în mod special valabil atunci când furnizorul de informații este o agenție străină.

În multe jurisdicții, au fost create rețele ale serviciilor de informații și de securitate (uneori denumite „centre de fuziune”), care au rolul de a agrega informații privind amenințările la adresa securității, furnizate de mai multe surse interne și externe. Unele din aceste rețele chiar permit agențiilor străine să facă schimburi de informații între ele. Organismele interne de supraveghere trebuie să aibă acces la informațiile culese și distribuite de aceste rețele pentru a putea înțelege pe deplin operațiunile agenției pe care sunt mandatate să o supravegheze – în special, dacă agenția în cauză oferă și primește informații de la astfel de instituții regionale, naționale și supranaționale.

Ca o reacție la volumul crescut al schimbului de informații atât pe plan intern, cât și cu agenții străine, au fost dispuse anchete *ad hoc* cu jurisdicție specială pentru examinarea schimbului de informații între mai multe agenții. Casetele 1 și 2 analizează exemple ale unor asemenea anchete *ad hoc* în Canada și Marea Britanie.

Serviciile de informații au evident nevoie să schimbe informații cu parteneri din ţară și din străinătate. Un serviciu care pur și simplu culege informații, fără a le comunica și altora, nu va reuși să-și îndeplinească obligația de a-i avertiza pe ceilalți în privința amenințărilor pe care le detectează. Natura transnațională a multora dintre amenințările actuale face necesară extinderea schimburilor de informații atât pe plan intern, cât și la nivel internațional.

Caseta 1: Anchetele ad hoc din Canada privind schimburile de informaţii

În conformitate cu rapoartele a două comisii multianuale de anchetă din Canada (Comisia de anchetă privind acțiunile oficialilor canadieni în cazul Maher Arar și Ancheta internă privind acțiunile oficialilor canadieni în cazul Abdullah Almalki, Ahmad Abou-Elmaati și Muayyed Nureddin), practicile poliției și ale serviciilor de informații canadiene privind schimbul de informații au contribuit indirect la torturarea unor cetățeni canadieni reținuți în Siria și Egipt, suspectați de terorism.[7] Ambele comisii erau organisme ad hoc, numite de guvern, în principal, ca reacție la scandalurile publice, dar și ca o recunoaștere crescândă a faptului că instituțiile de supraveghere existente, asociate fiind anumitor agenții, nu dispuneau de competența de a examina modul în care guvernul, în ansamblul său, reacționa la problemele majore de securitate internațională.

Ambele comisii au solicitat guvernelor american, egiptean și sirian să coopereze în cadrul anchetelor lor. Niciunul din cele trei guverne nu a dat curs solicitării. În plus, guvernul canadian a restricționat competența celor două comisii de a face publice informațiile secrete în a căror posesie intraseră. Totuși, deoarece aceste restricții au fost supuse unei examinări judiciare, comisiile au fost în măsură, în unele situații, să facă publice mai multe informații decât ar fi dorit guvernul – fie în urma unui litigiu câștigat, fie ca urmare a perspectivei unui asemenea litigiu. Comisiile au examinat unele detalii ale informațiilor pe care Canada le furnizase oficialilor din SUA, Siria și Egipt. Acestea includeau informații care făceau legătura între diverși cetățeni canadieni și grupări teroriste. Și anume, includeau liste de întrebări trimise de oficiali canadieni omologilor sirieni și egipteni, urmând ca întrebările respective să fie puse cetățenilor canadieni reținuți în Siria și Egipt ca fiind suspecţi de terorism.

Comisiile canadiene au analizat și informațiile primite de la respectivii oficiali străini, care au fost ulterior distribuite în interiorul Canadei și incluse în cel puțin o acțiune judiciară. Ambele comisii au descoperit deficiențe în ceea ce privește modalitățile în care au fost comunicate informațiile respective – nu numai la nivelul personalului din poliția locală, securitate, vamă și afaceri externe, dar și al agenților din străinătate.

Cele două anchete s-au axat, în principal, pe corectitudinea schimbului de informații, în special din punct de vedere al pericolelor la care au fost expuse drepturile omului, cum sunt dreptul de a nu fi supus torturii și dreptul la viață privată. Cu toate acestea, ar fi greșit să se concluzioneze că cele două comisii s-au opus creșterii schimbu-

[7] Comisia de anchetă privind acțiunile oficialilor canadieni în cazul Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* [*Raportul evenimentelor legate de cazul Maher Arar: analiză și recomandări*] (2006); și Anchetă internă privind acțiunile oficialilor canadieni în cazul Abdullah Almalki, Ahmad Abou-Elmaati și Muayyed Nureddin, *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin* [*Anchetă internă privind acțiunile oficialilor canadieni în cazul Abdullah Almalki, Ahmad Abou-Elmaati și Muayyed Nureddin*] (2008).

rilor de informații. Ele au dorit, pur și simplu, controale mai bune și verificări mai aprofundate. Comisia Arar a ajuns la concluzia că „schimbul de informații este vital, dar trebuie să se desfășoare într-o manieră sigură și responsabilă. Nevoia de a face schimb de informații nu înseamnă că informațiile trebuie comunicate fără control, îndeosebi fără folosirea unor avertismente. Și nici nu înseamnă că schimbul de informații trebuie realizat fără a lua în considerare cât de relevante, de sigure și de exacte sunt acestea sau fără a ține seama de legile care protejează informațiile personale ori drepturile omului." [8]

O a treia anchetă canadiană, care a examinat explozia în 1985 a unei bombe în avionul companiei Air India, a făcut o analiză a modului în care au fost comunicate informațiile dintr-o perspectivă întrucâtva diferită. Luând în considerare eficacitatea schimbului de informații (în contrapondere cu corectitudinea lor), Comisia Air India a formulat recomandări pentru diminuarea reticenței manifestate de serviciile de informații în ceea ce privește schimbul de informații cu poliția și cu celelalte agenții de aplicare a legii, din cauza riscului de divulgare a acestor informaţii. Toate cele trei comisii au recunoscut dilema fundamentală a schimbului de informații: dacă este prea limitat, e amenințată securitatea; dacă este prea extins, îndeosebi atunci când informațiile sunt furnizate fără un control, sunt amenințate drepturile omului.

Totuși, amplificarea schimbului de informații nu se produce fără inconveniente. Ea poate duce la încălcări ale dreptului la viață privată, precum și ale altor drepturi ale omului, în forme care nu sunt nici autorizate prin lege, nici justificate din punct de vedere etic. În același timp, există și riscul dezvăluirii unor informații secrete, obținute din surse sensibile.

Schimbul de informații prin intermediul rețelelor naționale și supranaționale (centre de fuziune) poate dilua și distorsiona responsabilitatea. Adesea, organismele parlamentare și specializate de supraveghere al căror mandat le limitează jurisdicția la o singură agenție nu dispun de acces la dosarele rețelelor din care fac parte serviciile de informații – un neajuns care poate împiedica serios activitatea de supraveghere.

Totodată, schimbul de informații dincolo de frontierele naționale poate genera conflicte în ceea ce privește politicile, precum în situația în care țări cu bune antecedente în domeniul drepturilor omului sunt presate să schimbe informații cu țări ale căror antecedente în materie sunt slabe. A schimba informații într-o asemenea situație poate face ca un stat să devină complice la abuzuri împotriva drepturilor omului, cum ar fi tortura, comise de partenerul său în schimbul de informații.

---

[8] Comisia de anchetă privind acțiunile oficialilor canadieni în cazul Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations*, p. 331.

Pe scurt, serviciile de informații nu și-ar putea desfășura activitatea dacă ar refuza întru totul să comunice informații; însă creșterea schimburilor de informații comportă numeroase riscuri. Cele care privesc indivizii, se referă la abuzuri împotriva drepturilor omului, în special, dreptul la viață privată. Riscurile pentru serviciile de informații includ diseminarea unor informații nesigure și/sau incorect obținute, care pot prejudicia reputația unui serviciu și pot avea ca rezultat alocarea defectuoasă a unor resurse insuficiente. Riscurile pentru organismele de supraveghere se referă la noi limitări ale capacității lor de a înțelege ce informații sunt furnizate și cum are loc schimbul de informații.

Caseta 2: O anchetă britanică ad hoc privind schimbul de informații

În 2010, guvernul britanic a inițiat o anchetă oficială (Ancheta privind deținuții) pentru a evalua măsura implicării britanice în relele tratamente la care au fost supuși deținuți aflați în alte țări.

La început, a fost pregătit un protocol care stipula că guvernul va furniza pentru anchetă toate informațiile relevante, exceptând situația în care furnizarea unor atari informații contravine obligațiilor existente în materie de confidențialitate.[9] De asemenea, protocolul a avut în vedere ca Secretarul Cabinetului să aibă ultimul cuvânt în ceea ce privește materialele ce puteau fi făcute publice. Scopul acestei prevederi era de a se asigura că nu va fi adus niciun prejudiciu interesului public prin dezvăluirea neautorizată a unor informații legate de securitatea națională, relațiile internaționale, apărare și economie. Un asemenea proces diferă semnificativ de procesul folosit de cele trei anchete canadiene amintite mai înainte, deoarece lipsește orice prevedere referitoare la examinarea judiciară a obiecțiilor guvernului față de dezvăluirea informațiilor. Ca urmare a acestor restricții și a altora, mai multe organizații pentru drepturile omului au refuzat să participe la anchetă.

În ianuarie 2012, guvernul britanic a întrerupt ancheta din cauza amânărilor continue, determinate de necesitatea de a aștepta concluzia cercetărilor penale – în privința unor activități pe care ancheta urma să le examineze – înainte ca ancheta să își poată începe munca. Deși această anchetă ad hoc de amploare ar fi putut fi un extraordinar exercițiu de supraveghere, faptul că guvernul britanic a recurs la astfel de măsuri discreționare și tranzitorii subliniază limitările cu care se confruntă structurile sale permanente de supraveghere.

[9] Ancheta privind deținuții, „Protocol for the Detainee Inquiry” [„Protocol pentru ancheta privind deținuții”] (2011) (disponibil la http://www.detaineeinquiry.org.uk/key-documents/protocol).

3. SUPRAVEGHEREA SCHIMBULUI DE INFORMAȚII CU AGENȚII STRĂINE

Schimbul de informații cu agenții străine prezintă, în general, cele mai mari provocări pentru organismele de supraveghere și cele mai mari riscuri pentru drepturile omului. Agențiile străine pot include servicii de informații, servicii de poliție și alte ramuri ale guvernelor străine care au acces la canale diplomatice de comunicare. Ele pot include și rețelele supranaționale din care fac parte una sau mai multe dintre aceste agenții. Un comentator a observat că, în contrast cu schimbul de informații pe plan intern, care poate fi supus unui control centralizat, „pe tărâmul internațional haotic … nu toate țările aderă la normele vieții private sau la alte libertăți fundamentale. Așadar, respectarea dreptului la viață privată se află la latitudinea fiecărei și oricărei agenții din rețea."[10]

Alte drepturi expuse riscului includ dreptul de a nu fi supus la tortură sau alte forme de tratament crud, neobișnuit sau degradant. După cum a observat Comisia Arar, „furnizarea către alte țări a informațiilor rezultate din investigațiile din Canada poate avea un efect «de undă» dincolo de frontierele canadiene, cu consecințe ce nu pot fi controlate din interiorul Canadei."[11] În cel mai rău scenariu posibil, informațiile trimise unei agenții străine pot fi utilizate de acea agenție în susținerea detenției extrajudiciare, a torturii și chiar a execuțiilor. Și invers, e posibil ca informațiile primite de la o agenție străină să fie obținute prin tortură sau denaturate în alte moduri.

Din rațiuni evidente, serviciile de informații și de poliție nu cunosc, în general, sursele și metodele utilizate de agențiile străine pentru a obține informațiile pe care, ulterior, le transmit. Ceea ce reprezintă o problemă, deoarece sursele și metodele folosite influențează atât corectitudinea informațiilor, cât și obligațiile celui care le primește de a respecta drepturile omului. În mod asemănător, furnizorii de informații nu cunosc utilizarea pe care o agenție externă o poate da informațiilor transmise. Uneori, agențiile furnizoare atașează informațiilor respective avertismente care restricționează utilizarea, însă nu dispun de nicio modalitate prin care să se asigure că partenerii străini vor ține seama de restricțiile respective. Schimbul de informații la nivel internațional se subsumează uneori suveranității statului și nevoii de a proteja caracterul secret al surselor, metodelor și utilizării informațiilor. Organismele interne de

[10] Francesca Bignami, „Toward a Right to Privacy in Transnational Intelligence Networks" [„Pentru dreptul la viață privată în rețelele transnaționale de informații"], în *Michigan Journal of International Law* 28, no. 3 (Primăvara 2007), p. 674.

[11] Comisia de anchetă privind acțiunile oficialilor canadieni în cazul Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* [*Un nou mecanism de verificare a activităților RCMP legate de securitatea națională*] (2006), p. 431.

supraveghere pot avea jurisdicție asupra agenției care transmite informațiile sau asupra celei care le primește, însă nu asupra amândurora atunci când una dintre ele este o agenție străină. Astfel că, în practică, aceste organisme pot supraveghea doar una din părțile implicate în operațiunea de schimb.

3.1 PRACTICI GREȘITE ÎN SCHIMBUL DE INFORMAȚII LA NIVEL INTERNAȚIONAL

Cel mai notoriu exemplu recent de practică greșită în schimbul de informații pe plan internațional a fost cazul Maher Arar. În urma atacurilor din 11 septembrie 2001, investigatorii din cadrul Poliției Regale Călare din Canada (RCMP), care au efectuat cercetări pe teren, au furnizat unor oficiali din guvernul SUA conținutul unei baze de date de investigare. Nici una dintre informații nu a fost verificată în prealabil pentru a se determina cât este de sigură și de relevantă, iar RCMP nu a impus nicio restricție cu privire la utilizarea lor. Ulterior, o comisie canadiană de anchetă a stabilit faptul că informațiile în cauză au jucat, probabil, un rol în reținerea domnului Arar de către SUA și, apoi, în extrădarea lui în Siria, unde a fost torturat. În mod semnificativ, comisia nu a ajuns la nicio constatare definitivă, fiindcă nici guvernul SUA, nici cel sirian nu au cooperat cu ancheta întreprinsă. Confruntat cu aserțiuni referitoare la suveranitatea statului, un organism de supraveghere poate face prea puțin pentru a aprofunda problematica schimbului de informații secrete la nivel internațional. Cu toate acestea, atât Comisia Arar, cât și ancheta, care a urmat, privind reținerea de către Siria și Egipt a altor trei cetățeni canadieni, au constatat că întrebările trimise autorităților siriene și egiptene de către RCMP și Serviciul Canadian pentru Informații de Securitate au contribuit la torturarea deținuților de către agenții sirieni și egipteni.

Asemenea constatări reprezintă lecții importante de precauție în privința a ceea ce trebuie evitat. Ele avertizează că serviciile de informații, chiar dacă se confruntă cu circumstanțe urgente, trebuie să verifice cu atenție informațiile înainte de a le furniza unor parteneri străini. Totodată, dacă e cazul, ele trebuie să atașeze avertismente unor informații și să stabilească restricții în utilizarea informaţiilor. În plus, serviciile trebuie să se abțină de la a trimite cereri pentru continuarea investigării, precum liste de întrebări, către parteneri străini, ai căror anchetatori se știe că practică tortura sau alte forme de abuzuri împotriva drepturilor omului.

3.2 BUNE PRACTICI ALE SERVICIILOR DE INFORMAȚII ÎN SCHIMBUL DE INFORMAȚII LA NIVEL INTERNAȚIONAL

Ce este o bună practică în schimbul de informații la nivel internațional? Pentru început, agențiile implicate trebuie să se asigure că sunt bine informate cu pri-

vire la partenerii cu care fac schimb de informații. Raportorul special al Națiunilor Unite pentru promovarea și protejarea drepturilor omului și libertăților fundamentale în contextul combaterii terorismului a recomandat ca „înainte de a iniția un acord de schimb de informații sau de a transmite informații pe baze *ad hoc*, serviciile de informații să facă o evaluare a antecedentelor partenerului în ceea ce privește drepturile omului și protecția datelor, precum și a măsurilor legale de siguranță și a mecanismelor instituționale de control care guvernează activitatea partenerului. Înainte de a transmite informații, serviciile de informații (trebuie) să se asigure că orice informații furnizate sunt relevante pentru mandatul primitorului, că vor fi folosite în conformitate cu condițiile specificate și că nu vor fi întrebuințate în scopuri ce încalcă drepturile omului."[12] Deși raportorul special a adresat această recomandare serviciilor de informații, ea are relevanță și pentru organismele de supraveghere, a căror datorie este de a asigura respectarea bunelor practici și posibilitatea de recurs dacă acest lucru nu se întâmplă.

Comisia Arar a constatat că RCMP nu a avut informații adecvate despre practicile forțelor de securitate siriene și egiptene atunci când a decis să le furnizeze acestora informații. În general, dintre agențiile care fac schimb de informații pe plan internațional, forțele de poliție au cea mai redusă expertiză în evaluarea practicilor partenerilor străini. În consecință, ar fi prudent ca agențiile interne care fac schimb de informații pe plan internațional să creeze și să mențină o bază de date comună, care să includă date la zi despre potențialii parteneri străini. În acest fel, agențiile interne ar putea lua decizii în cunoștință de cauză privind furnizarea anumitor informații. O astfel de abordare ar ameliora procesul decizional în ceea ce privește nu numai transmiterea de informații, ci și evaluarea informațiilor primite. În exemplele anterioare din Canada, informațiile au rezultat în urma unor interogatorii brutale și au fost ulterior distribuite pe scară largă oficialilor din agențiile de aplicare a legii și de informații și din domeniul afacerilor externe. După cum a conchis Comisia

---

[12] Consiliul Națiunilor Unite pentru Drepturile Omului, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight* [*Raportul Raportorului Special pentru promovarea și protejarea drepturilor omului și libertăților fundamentale în contextul combaterii terorismului: Compilație de bune practici privind cadrul și măsurile legale și instituționale, care asigură respectarea drepturilor omului de către agențiile de informații în contextul luptei împotriva terorismului, inclusiv supravegherea acestora*], United Nations Document A/HRC/14/46 (17 mai 2010), p. 46.

Arar, „Nu are niciun sens ca agenții diferite să opereze pe baza unor evaluări diferite ale acelorași informații primite din partea unui guvern străin.”[13]

Totodată, așa cum s-a arătat mai înainte, este imperios necesar ca serviciile de informații să atașeze avertismente informațiilor pe care le furnizează unor entități din străinătate, prin care să restricționeze utilizarea acestora. Cu toate că nu există nicio garanție privind respectarea de către guvernele străine a acestor avertismente, există bune practici care măresc probabilitatea că se va ține seama de ele – și, dacă nu sunt luate în considerare, asemenea practici pot îmbunătăți șansele ca abaterile să fie remediate. Comisia Arar a făcut mai multe recomandări în această privință. Mai întâi, avertismentele trebuie să fie formulate cât mai clar și precis. De exemplu, a permite unui guvern să distribuie informațiile primite în cadrul „comunității sale de informații” îi oferă acestuia posibilitatea de a-și extinde prea mult mandatul, ținând seama de numărul mare de agenții care pot fi incluse într-un concept atât de vag. În al doilea rând, trebuie să li se interzică guvernelor primitoare să folosească informațiile ce le-au fost furnizate în cadrul unor proceduri judiciare, fie ele penale sau referitoare la imigrație ori extrădare. Mai mult, trebuie să se anexeze întotdeauna un avertisment prin care se solicită guvernelor primitoare să contacteze anumiți oficiali din guvernul care a furnizat informații în situația în care doresc să modifice un avertisment sau să raporteze un abuz. În acest mod, s-ar înlocui actuala practică greșită în care o astfel de solicitare e adresată vag către agenția sau guvernul care transmite datele în cauză și s-ar întări responsabilitatea individuală. Potrivit Comisiei Arar, „un avertisment poate contribui la stabilirea unor canale corespunzătoare pentru o comunicare clară cu privire la utilizarea și distribuirea informațiilor la care se referă acel avertisment.”[14] În fine, întotdeauna trebuie anexat un avertisment prin care se solicită agenției primitoare să respecte reglementările privind informațiile cu caracter personal, impuse de legislația din jurisdicția furnizorilor de informații, precum și pe acelea care se aplică în jurisdicția celor care le primesc.[15]

Dacă un serviciu de informații sau de securitate află că unul din avertismentele sale a fost încălcat, trebuie să adreseze imediat o reclamație agenției respective. În funcție de gravitatea abuzului, agenția care a transmis informațiile ar

---

[13] Comisia de anchetă privind acțiunile oficialilor canadieni în cazul Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations*, p. 349.

[14] Ibid., p. 342.

[15] Hans Born și Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practices for Oversight of Intelligence Agencies* [*Responsabilizarea în domeniul intelligence: standarde legale și cele mai bune practici pentru supravegherea agențiilor de informații*] (Geneva: DCAF, Universitatea din Durham și Parlamentul Norvegiei, 2005), p. 45.

putea să reconsidere măsura în care se justifică acordul în baza căruia s-a făcut schimbul de informații. În același timp, trebuie să se aducă la cunoștința organismelor de supraveghere fiecare încălcare, precum și reacția agenției care a transmis informațiile. Organismele de supraveghere pot avea un rol important în asigurarea faptului că agențiile pe care le supraveghează cer respectarea avertismentelor și iau măsurile corespunzătoare de remediere când este necesar.

După cum sugerează constatările Comisiei Arar, trebuie să se acorde o atenție specială atunci când se transmit întrebări agențiilor străine nu numai pentru că acestea ar putea să ducă la folosirea unor tactici dure de interogare, dar și pentru că agențiile străine ar putea folosi astfel de întrebări într-un mod chiar și mai puțin controlabil printr-un avertisment. „Informațiile," după cum a conchis Comisia Arar, „nu trebuie niciodată furnizate unei țări străine în care există un risc verosimil că vor conduce sau contribui la utilizarea torturii."[16] Raportorul special al Națiunilor Unite a făcut recomandări similare, subliniind că organismele de supraveghere trebuie să acorde o atenție deosebită conduitei care ar putea încălca drepturile omului. În plus, el a recomandat ca angajații serviciilor de informații, care au primit dispoziții să participe la acțiuni ce încalcă drepturile omului, să fie autorizați să refuze dispozițiile respective și să înainteze reclamații organismelor de supraveghere.[17]

Schimbul de informații cu parteneri din străinătate trebuie să fie întotdeauna bine documentat din cauza riscurilor pe care le implică și, totodată, pentru a facilita verificarea și supravegherea. Secțiunea 17 a „Legii privind Serviciul Canadian pentru Informații de Securitate" acordă ministrului pentru siguranța publică (în consultare cu ministrul afacerilor externe) autoritatea legală de a încheia acorduri de cooperare cu agenții și guverne străine. În absența unui astfel de acord, CSIS nu poate să furnizeze legal informații unei entități din străinătate. (Totuși, poate primi informații.)[18] O directivă ministerială adițională impune ca RCMP să încheie acorduri scrise specifice cu partenerii săi de schimb de informații. Aceste acorduri trebuie susținute cu avize juridice și, în cazul agențiilor străine, cu avize de politică externă. Chiar și așa, Comisia

[16] Comisia de anchetă privind acțiunile oficialilor canadieni în cazul Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations*, p. 345.

[17] Consiliul Națiunilor Unite pentru Drepturile Omului, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*.

[18] Anchetă internă privind acțiunile oficialilor canadieni în cazul Abdullah Almalki, Ahmad Abou-Elmaati și Muayyed Nureddin, *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin*, p. 82.

Arar a constatat că RCMP nu a aplicat această directivă în activitatea curentă de schimb de informații. Comisia a ajuns la concluzia că, deși acordurile scrise „nu trebuie să fie excesiv de formale sau detaliate,” ele pot spori sensibilitatea agenților față de nevoia de a respecta avertismentele și drepturile omului atunci când fac schimb de informații.[19]

Verificarea antecedentelor are o importanță specială atunci când un serviciu de informații încheie un acord de cooperare cu un partener străin care are un istoric discutabil în privința drepturilor omului. Atunci când informațiile sunt transmise unui astfel de partener, Comisia Arar a recomandat ca agenția furnizoare să aibă o evidență în scris a informațiilor comunicate și a motivației care a stat la baza deciziei de a le transmite.[20] În continuare, comisia a recomandat ca o abordare similară să fie adoptată și în cazul primirii de informații din partea unor țări cu antecedente discutabile în privința drepturilor omului:

> În materie de responsabilitate, este important ca procesul decizional să fie prezentat clar în scris, iar responsabilii pentru luarea deciziilor să fie specificați. În plus, deciziile de a primi informații din partea unor țări cu antecedente discutabile în privința drepturilor omului trebuie să fie verificate de organismul corespunzător de verificare.[21]

3.3 BUNE PRACTICI ALE ORGANISMELOR DE SUPRAVEGHERE CU PRIVIRE LA SCHIMBUL DE INFORMAȚII ÎNTRE AGENȚII LA NIVEL INTERNAȚIONAL

Este extrem de important ca organismele de supraveghere să aibă acces la informațiile furnizate de agențiile pe care le supraveghează, indiferent dacă aceste informații sunt secrete, sau nu. Printre bunele practici recomandate de raportorul special al Națiunilor Unite, este aceea ca „instituțiile independente de supraveghere să fie în măsură să examineze acordurile privind schimburile de informații, precum și orice informații transmise de serviciile de informații unor entități străine.”[22] În fapt, potrivit raportorului special al Națiunilor Unite, „o bună practică pentru legislația națională este de a solicita explicit serviciilor de informații să prezinte unui organism independent de supraveghere rapoarte referitoare la schimbul de informații.”[23]

---

[19] Comisia de anchetă privind acțiunile oficialilor canadieni în cazul Maher Arar, *Report of the Events Relating to Maher Arar*, p. 322.

[20] Ibid., p. 347.

[21] Ibid., p. 348.

[22] Consiliul Națiunilor Unite pentru Drepturile Omului, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, p. 48.

[23] Ibid., p. 49.

O posibilă barieră în calea unei supravegheri eficace este regula terței părți, un avertisment asociat frecvent informațiilor transmise, care restricționează distribuirea acestora altor entități („terțe părți”). Unele țări, precum Germania, nu acordă organismelor de supraveghere acces la informațiile transmise, deoarece organismele respective sunt considerate a fi terțe părți.

O reacție serioasă la o asemenea interpretare a regulii terței părți ar fi ca organismele de supraveghere să insiste asupra faptului că, în ceea ce privește schimbul de informații cu entități din străinătate, ele pot fi considerate ca făcând parte din serviciul care primește informațiile din afara ţării. Serviciile de informații se pot opune unei poziții de acest gen, temându-se că serviciile străine vor fi mai puțin dornice să facă schimb de informații cu ele. Însă pot fi

Caseta 3: Supravegherea schimbului de informații cu străinătatea de către Comisia olandeză de Verificare a Serviciilor de Informații și de Securitate

În 2002, guvernul olandez a înființat un organism permanent, cu atribuții de supraveghere a unei palete largi de aspecte din domeniul intelligence, având inclusiv jurisdicția de a verifica operațiunile mai multor servicii de informații și de a accesa informațiile secrete necesare efectuării unor astfel de verificări. În 2009, această Comisie de Verificare a Serviciilor de Informații și de Securitate a publicat un raport amplu referitor la cooperarea olandeză cu serviciile străine, care a vizat politicile și practicile unui singur serviciu olandez de informații între anul 2002 și jumătatea anului 2005.

Raportul a constatat că serviciul olandez de informații și departamentul său de afaceri externe nu au urmărit cu suficientă atenție dacă partenerii străini, inclusiv cei cu antecedente de încălcare a drepturilor omului, au respectat un standard adecvat pentru schimbul de informații. Raportul a mai constatat că serviciile olandeze de informații acționaseră ilegal, furnizând date cu caracter personal partenerilor străini. El a recomandat ca aceste servicii să întrerupă schimbul de informații cu partenerii străini pe care îi suspectează că ar putea întrebuința informațiile în scopuri ilegale.[24] Raportul a mai recomandat punerea în aplicare a unui proces structurat, prin care să se determine oportunitatea încheierii unor acorduri de schimb de informații cu servicii străine. Asemenea acorduri trebuie să fie supuse unei verificări periodice și trebuie să prevadă păstrarea unor evidențe scrise cu toate informațiile personale care au făcut obiectul schimbului.[25]

[24] Olanda, Comisia de Verificare a Serviciilor de Informații și de Securitate (CTIVD), *Review Report on the cooperation of the GISS with foreign intelligence and/or security services* [*Raportul de verificare a cooperării GISS cu serviciile de informații și/sau de securitate străine*], CTIVD Nr. 22A (12 august 2009) (disponibil la: http://www.ctivd.nl/?English), Secțiunea 14.2.

[25] Ibid., Secțiunile 14.6 și 14.15.

încurajate să-și informeze partenerii din străinătate cu privire la responsabilitatea lor de a coopera cu organismele de supraveghere, care, în multe cazuri, urmează aceleași proceduri de secretizare ca și agenția care primeşte informaţiile.

De asemenea, organismele de supraveghere trebuie să fie conștiente că serviciile de informații utilizează uneori schimbul de informații ca pe un mijloc de a evita restricțiile interne la adresa activităților lor. Abordând această problemă, raportorul special al Națiunilor Unite a propus o bună practică, bazată pe un raport al Parlamentului European cu privire la sistemul ECHELON de informații provenite din semnale, și anume că „serviciilor de informații li se interzice explicit să folosească asistența din partea serviciilor omoloage din străinătate în orice mod care duce la eludarea normelor legale naționale și a controalelor instituționale asupra propriilor activități.” [26]

În fine, organismele de supraveghere trebuie să adopte și/ori să încurajeze aceleași bune practici în schimbul de informații pe care le recomandă serviciilor de informații aflate în sarcina lor. De pildă, organismele de supraveghere trebuie să se informeze ele însele cu privire la antecedentele partenerilor străini în materia drepturilor ale omului. În mod similar, trebuie să încurajeze agențiile pe care le supraveghează să încheie în scris acorduri formale cu partenerii străini.

3.4 BUNE PRACTICI ALE ORGANISMELOR DE SUPRAVEGHERE CU PRIVIRE LA SCHIMBUL DE INFORMAȚII PRIN INTERMEDIUL REȚELELOR

Dat fiind că schimbul internațional de informații poate avea loc în plan multilateral, ca și în plan bilateral, organismele de supraveghere trebuie să se poziționeze astfel, încât să poată minimiza provocările și să maximizeze oportunitățile ce decurg din schimbul de informații prin intermediul rețelelor. De exemplu, rețelele de schimburi de informații pot efectua evaluări ale agențiilor partenere cu privire la respectarea drepturilor omului; această modalitate de evaluare poate fi preferabilă în raport cu evaluările similare făcute de agenții individuale. De asemenea, rețelele pot exercita o influență mai mare decât agențiile individuale atunci când se pune problema aplicării avertismentelor referitoare la drepturile omului şi viaţa privată, care însoțesc multe schimburi de informații.[27] În fine, rețelele au potențialul de a disemina bune practici referitoare la informațiile sigure și supraveghere, prin faptul că

[26] Ibid., pp. 49–50.
[27] Bignami, „Toward a Right to Privacy in Transnational Intelligence Networks,” pp. 683-684.

cer agențiilor membre să respecte standardele impuse de acei membri care utilizează cele mai bune practici.

Unele dintre rețelele europene de schimburi de informații, așa cum sunt cele conduse de Europol și Clubul de la Berna, au impus într-adevăr standarde înalte, care s-au dovedit benefice. În plus, ele au încurajat unele state să recurgă la un schimb bilateral de informații, mai puțin formal (sau chiar de la caz la caz).[28] Pentru a contracara o asemenea tendință, organismele de supraveghere trebuie să folosească o dublă abordare, subliniind beneficiile schimbului de informații în cadrul rețelelor multilaterale și urmărind, în același timp, cu multă atenție schimburile de informații care au loc pe baza înțelegerilor bilaterale mai puțin transparente. Deși poate fi dificilă obținerea unor date despre partenerii străini cu care un serviciu intern face schimb de informații, organismele de supraveghere au nevoie de aceste date și trebuie să monitorizeze acordurile și practicile privind schimbul de informații cu parteneri străini.

Pentru țările în curs de dezvoltare, resursele aflate la dispoziția membrilor rețelelor internaționale de schimburi de informații reprezintă un stimulent puternic pentru a se alătura acestor rețele, chiar dacă alăturarea impune respectarea anumitor norme referitoare la drepturile omului. Organismele de supraveghere pot avea un rol important în promovarea afilierii dacă devin ele însele conștiente de standardele ce trebuie atinse și încurajează serviciile de informații pe care le supraveghează să le respecte.

4. SUPRAVEGHEREA SCHIMBULUI DE INFORMAȚII CU AGENȚII INTERNE

După cum s-a discutat mai înainte, ca urmare a atacurilor din 11 septembrie 2001, multe guverne au extins schimburile de informații între partenerii interni – inclusiv oficiali din domeniul intelligence, din poliție și poliție de frontieră, din vamă și din transporturi –, convinse fiind că această măsură va contribui la prevenirea unor viitoare atacuri teroriste. În Marea Britanie, de exemplu, Secțiunea 19 din „Legea privind terorismul” din 2008 a acordat serviciilor britanice de informații o mare libertate de decizie în privința schimbului de informații. Legea a autorizat în mod expres orice persoană să dezvăluie informații serviciilor de informații. Legea a autorizat, de asemenea, serviciile de informații să dezvăluie informații în funcție de necesități, pentru îndeplinirea corespunzătoare a funcțiilor lor, pentru prevenirea sau depistarea unor

[28] Anchetă internă privind acțiunile oficialilor canadieni în cazul Abdullah Almalki, Ahmad Abou-Elmaati și Muayyed Nureddin, *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin*, p. 68.

infracțiuni grave și pentru susținerea proceselor penale. Astfel, presiunea recentă în favoarea creșterii schimburilor de informații a condus la dezvăluirea unui volum mai mare de informații privind nu numai amenințările potențiale la adresa securității, dar și prevenirea criminalității și cercetările penale.

4.1 PROVOCĂRI PENTRU SCHIMBUL DE INFORMAȚII PE PLAN INTERN

Din perspectiva activității de supraveghere, dezvăluirea informațiilor către parteneri interni generează multe dintre preocupările de același gen prezentate anterior în legătură cu schimbul de informații la nivel internațional. Există, însă, și unele preocupări în plus, specifice schimbului de informații pe plan intern. Cea mai importantă dintre ele este pericolul ca limitările jurisdicționale să împiedice o verificare eficace, coordonată, a schimbului de informații pe plan intern, deoarece respectivele organisme de supraveghere nu au autoritatea legală de a verifica toate agențiile interne implicate. Atunci când competențele de supraveghere sunt deficitare din acest punct de vedere, răspunderea se diluează și se creează breșe prin care schimburile de informații pot avea loc fără o verificare adecvată.

Dat fiind că serviciile de informații dispun de puteri speciale, guvernele naționale le supun, de regulă, unei supravegheri mai intense decât cea impusă agențiilor de aplicare a legii. Acolo unde se ivesc breșe de responsabilitate, această supraveghere intensificată poate fi compromisă. De pildă, atunci când guvernul canadian a decis să investigheze acțiunile oficialilor canadieni cu privire la torturarea lui Maher Arar și a celorlalți cetățeni canadieni în Siria și Egipt, a constatat că jurisdicția de supraveghere a Comisiei de Verificare a Informațiilor de Securitate nu se extindea și la oficialii din poliție, din vamă și din domeniile afacerilor externe și al imigrării, care fuseseră implicați în schimbul de informații cu Siria și Egiptul. Drept rezultat, guvernul a trebuit să facă anchete temporare, *ad hoc*, pentru a acoperi breșa de responsabilitate.

Și federalismul poate duce la existența unor breșe periculoase de responsabilitate. De exemplu, în SUA, după 11 septembrie 2001, au fost înființate centre de fuziune pentru a promova schimbul de informații între agențiile federale, statale și municipale. S-a insistat pe ideea că nu sunt necesare noi mecanisme de supraveghere, deoarece fiecare agenție participantă a rămas în sfera de acțiune a unei structuri de supraveghere deja existente. Acest argument nu recunoștea, totuși, că, din punct de vedere practic, organismele de supraveghere asociate unui anumit nivel de guvernare dispun rareori de jurisdicția ne-

cesară pentru a verifica acțiunile întreprinse de agenții situate pe alte niveluri de guvernare.[29]

4.2 PRACTICI GREȘITE ÎN SCHIMBUL DE INFORMAȚII PE PLAN INTERN

Începând cu 11 septembrie 2001, o practică deosebit de greșită în schimbul de informații pe plan intern a fost identificarea incorectă a protestatarilor nonviolenți ca suspecți de terorism. În SUA, mai multe centre de fuziune s-au făcut vinovate de o asemenea practică. Deoarece identificarea incorectă s-a produs după contopirea diverselor baze de date furnizate de agențiile federale, statale și locale, care conţineau informații strategice referitoare la amenințări teroriste și vulnerabilități, agențiile participante fie au invocat necunoașterea, fie au învinovățit pe altcineva pentru informațiile nefundamentate. Unele centre de fuziune au complicat problema refuzând să pună la dispoziția organismelor de supraveghere înregistrări ale modului în care au fost adunate informațiile.[30] Acești factori, combinați, fac foarte dificilă tragerea la răspundere a centrelor de fuziune și a agențiilor participante pentru activitățile desfășurate.

Dintr-o perspectivă mai generală, rețelele de informații și agențiile care fac parte din acestea trebuie să restrângă schimbul fără discernământ al informațiilor posibil nesigure. În Canada, informații nesigure, obținute de la o agenție străină de către Departamentul Afacerilor Externe, au fost ulterior distribuite agențiilor interne de informații și de aplicare a legii, fără a se constata vreo preocupare privind temeinicia lor. Mai mult, informațiile au fost folosite ca bază pentru obținerea unui mandat de percheziționare. În felul acesta, practicile greșite în schimbul de informații pe plan intern pot multiplica pericolele inerente ce decurg din schimbul de informații cu străinătatea.

4.3 BUNE PRACTICI ÎN SCHIMBUL DE INFORMAȚII PE PLAN INTERN

O bună practică în schimbul de informații pe plan intern începe cu păstrarea unor evidențe permanente, care urmăresc traseul informațiilor deținute și distribuite de centrele de fuziune și celelalte entități care facilitează schimbul de informații. În absența unor asemenea evidențe și a pistelor de control pe care le asigură, supravegherea schimbului de informații pe plan intern ar fi dificilă, dacă nu chiar imposibilă.

---

[29] Danielle Citron și Frank Pasquale, „Network Accountability for the Domestic Intelligence Apparatus" [„Responsabilitatea rețelei în raport cu aparatul intern de informații"], în *Hastings Law Journal* 62 (2011), p. 1441.

[30] Ibid.

Avertismentele reprezintă și ele o bună practică în schimbul de informații pe plan intern, ca și în cazul schimbului de informații la nivel internațional, îndeosebi atunci când informațiile care fac obiectul schimbului urmează să fie folosite pentru aplicarea legii. Agenția furnizoare trebuie să analizeze atent dacă informațiile care urmează a fi transmise sunt îndeajuns de sigure pentru a putea fi folosite în scopul aplicării legii și, în același timp, dacă are dreptul legal de a comunica informații în acest scop. Raportorul special al Națiunilor Unite a subliniat necesitatea ca țările să adopte baza legală pentru schimbul de informații pe plan intern. Secțiunea 19 a „Legii privind terorismul" din Marea Britanie din anul 2008 oferă un exemplu în acest sens.

Crearea unei baze legale poate oferi legislatorilor oportunitatea de a reflecta cu privire la relevanța mecanismelor de supraveghere existente și, poate, de a face modificări în structura de supraveghere existentă. De pildă, după examinarea bazei legale a activității de supraveghere din Canada, Comisia Arar a recomandat forului legislativ canadian să creeze „pasarele legislative" care să permită diferitelor organisme de supraveghere să facă schimb de informații secrete și să conlucreze pentru verificarea activităților legate de securitatea națională. Recomandarea comisiei s-a întemeiat pe principiul solid conform căruia o supraveghere trebuie să țină pasul cu activitățile supravegheate. Cu alte cuvinte, în cazul extinderii autorizării legale pentru schimbul de informații, aceeași extindere trebuie aplicată și competențelor de verificare.

Unii comentatori au pledat pentru necesitatea unei forme distincte de „responsabilizare a rețelelor," pentru ca organismele de supraveghere să țină pasul cu proliferarea rețelelor interne de schimburi de informații. În acest sens, s-a recomandat înregistrarea și păstrarea tuturor informațiilor primite și transmise (în așa fel, încât organismele de supraveghere să poată crea piste de control sigure) și înființarea, în cadrul centrelor de fuziune, a unor mecanisme de corectare (astfel încât să se poată remedia transmiterea informațiilor inexacte și încălcarea drepturilor la viața privată).[31] Alți comentatori au accentuat necesitatea ca inspectorii generali, îndeosebi în SUA, să desfășoare anchete comune privind practicile utilizate în schimbul de informații de agențiile pe care le supraveghează.[32] În mod asemănător, în Canada, Comisia Arar a reco-

---

[31] Ibid.

[32] Philip Heymann și Juliette Kayyem, *Preserving Liberty in the Face of Terror* [*Păstrarea libertății în fața terorii*] (Boston: MIT Press, 2005); Kent Roach, „Review and Oversight of National Security Activities and Some Reflections on Canada's Arar Inquiry" [„Verificarea și supravegherea activităților de securitate națională și câteva reflecții privind Ancheta Arar din Canada"], în *Cardozo Law Review* 29, no. 1 (octombrie 2007), pp. 53–84.

mandat ca jurisdicția organismelor de supraveghere a serviciilor de informații să fie extinsă pentru a include o serie de agenții care și-au asumat noi și importante responsabilități privind securitatea după evenimentele din 11 septembrie 2001.[33] În Belgia, organismelor distincte care supraveghează poliția și, respectiv, serviciile de informații li se permite deja să facă schimb de informații; totodată, aceste organisme au efectuat mai multe anchete comune.[34]

În absența unor astfel de mecanisme extinse de supraveghere, guvernele care doresc să investigheze acțiunile mai multor agenții interne, implicate în schimbul de informații de securitate, trebuie să inițieze anchete *ad hoc*, precum Comisia Arar, deoarece nici unul dintre organismele de supraveghere nu dispune de mandatul necesar pentru a verifica acțiunile mai multor agenții. Totuși, numirea unui organism *ad hoc*, dat fiind că este discreționară și are caracter extraordinar, nu poate reprezenta un substitut pentru un organism permanent de supraveghere, cu suficient de multă autoritate pentru a efectua o verificare de substanță. Din acest motiv, Comisia Arar a recomandat ca organismelor permanente de supraveghere, care au misiunea de a verifica acțiunile agențiilor canadiene de informații și de aplicare a legii, să li se acorde o autoritate sporită de verificare a acțiunilor unei serii de agenții cu care se face schimb de informații de securitate. Din păcate, această recomandare, precum și recomandarea ca guvernul să creeze căi legale pentru supravegherea în comun – ambele emise în 2006 – nu au fost încă implementate.[35]

În SUA, a fost înregistrat un oarecare progres în ceea ce privește învestirea structurilor permanente de responsabilizare cu competența de a examina mai multe agenții interne care participă actualmente la schimbul de informații de securitate. Un exemplu este ancheta privind interceptările telefonice neautorizate, desfășurată în comun de inspectorii generali din Departamentul Apărării, Departamentul de Justiție, CIA, Agenția Națională de Securitate și Oficiul Directorului pentru Informații Naționale.[36]

---

33 Comisia de anchetă privind acțiunile oficialilor canadieni în cazul Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities*.

34 Ibid., pp. 333–334.

35 Kent Roach, *The 9/11 Effect: Comparative Counter-Terrorism* [*Efectul 11 septembrie: abordare comparativă a luptei împotriva terorismului*] (Cambridge: Cambridge University Press, 2011), pp. 416–420 și 455–459.

36 Oficiile inspectorilor generali din Departamentul Apărării, Departamentul de Justiție, CIA, Agenția Națională de Securitate și Oficiul Directorului pentru Informații Naționale, *Unclassified Report on the President's Surveillance Program* [*Raport neclasificat privind Programul de Supraveghere al Președintelui*] (10 iulie 2009).

Caseta 4: Verificarea schimbului de informaţii pe plan intern printr-o anchetă privind serviciile australiene de informații

Australia a făcut progrese semnificative în adaptarea activității de supraveghere a serviciilor de informaţii cu scopul de a respecta cerințele noii abordări „la nivelul întregului guvern” a problemelor legate de securitate și de schimbul de informații. O anchetă australiană în domeniul intelligence a recomandat, în 2006, extinderea mandatelor inspectorului general, un organism specializat de supraveghere, și, respectiv, al comisiei parlamentare comune competente, pentru ca acestea să aibă posibilitatea de a supraveghea acțiunile tuturor serviciilor interne de informații.[37]

Deși o astfel de recomandare denotă recunoașterea faptului că volumul schimburilor de informații între serviciile interne a crescut, ea a acordat mai puțină atenție schimbului de informații între serviciile interne și alte agenții interne. Această deficiență a fost corectată în 2010, când parlamentul australian a adoptat o lege care acordă inspectorului general autoritatea de a examina toate chestiunile referitoare la securitate și informații din cadrul oricărui departament federal sau al oricărei agenții federale.[38] Cu toate acestea, într-o privință, noua lege nu a fost nici pe departe de dorit. Deși raportorul special al Națiunilor Unite a subliniat că este important ca organismele de supraveghere să aibă capacitatea de a iniția propriile lor verificări, noua lege australiană a impus ca extinderea puterilor inspectorului general să se facă pe baza unui mandat din partea primului ministru.[39]

Între timp, Australia a înființat noi comisii parlamentare pentru a verifica acțiunile agențiilor de aplicare a legii, implicate în domeniul securității naționale și în schimbul de informații. Totodată, a mărit dimensiunile comisiei parlamentare comune, însărcinate cu supravegherea serviciilor de informații.

5. RECOMANDĂRI

Următoarele recomandări sunt menite a facilita supravegherea schimbului de informații realizat pe plan intern și internațional. Ele se adresează nu numai organismelor de supraveghere din ramurile legislativă și executivă, dar și servi-

---

37 Philip Flood, *Report of the Inquiry into Australian Intelligence Agencies* [*Raportul anchetei privind agențiile australiene de informații*] (Canberra: Government of Australia, 2004).

38 Australia, National Security Legislation Amendment Act No. 127 [Legea nr.127 pentru amendarea legislației privind securitatea națională], din 2010, capitolul 9; a se vedea și Kent Roach, *The 9/11 Effect: Comparative Counter-Terrorism* [*Efectul 11 septembrie: abordare comparativă a luptei împotriva terorismului*] (Cambridge: Cambridge University Press, 2011), pp. 354–356.

39 Consiliul Națiunilor Unite pentru Drepturile Omului, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*.

ciilor de informații supravegheate și altor entități implicate în răspunsurile „la nivelul întregului guvern” în fața amenințărilor la adresa securității.

Deoarece schimbul de informații trebuie să aibă loc, e necesar să fie efectuat într-o manieră autorizată prin lege și care respectă drepturile omului, inclusiv dreptul la viață privată. Pentru asigurarea acestor condiții, este important să se ofere organismelor de supraveghere resursele legale și alte resurse de care au nevoie pentru a ține pasul cu volumul în creștere al schimburilor de informații în plan intern și internațional, care se manifestă în lumea de după 11 septembrie 2001.

Dezvoltarea unor linii directoare interne privind schimbul de informații

Serviciile de informații trebuie să conceapă un set de principii care să reglementeze practicile lor în schimbul de informații. Principiile trebuie să fie stabilite în scris, sub forma unei legi sau a unei politici. Ele trebuie:

- să impună respectarea drepturilor omului (inclusiv evitarea complicității la tortură) și respectarea legilor ce reglementează viața privată (inclusiv schimbul de informații cu caracter personal).

În special, principiile trebuie să interzică schimbul de informații atunci când există un risc plauzibil ca acesta să determine sau să contribuie la practicarea torturii.

- să impună verificarea informațiilor care fac obiectul schimbului (trimise ori primite) din punctul de vedere al relevanței, solidității, exactității și al impactului asupra vieții private și asupra celorlalte drepturi ale omului.
- să recunoască necesitatea de a atașa avertismente la informațiile care sunt trimise, precum și de a respecta avertismentele atașate de celelalte părți la informațiile care sunt primite – rolul avertismentelor fiind acela de a se asigura că informațiile nu sunt utilizate în scopuri incorecte sau într-o manieră incorectă, care încalcă legislația internă ori pe cea internațională.
- să recunoască obligația permanentă de a corecta informațiile eronate trimise altor agenții și de a efectua evaluări independente referitoare la temeinicia informațiilor primite de la alții.
- să includă un angajament privind realizarea schimbului de informații într-un mod care să faciliteze stabilirea responsabilităților în cadrul serviciului care furnizează informațiile și în raport cu organismele de supraveghere. Și anume, informațiile transmise și primite trebuie înregistrate în scris, iar pistele de control trebuie să descrie modul în care s-a autorizat schimbul de informații și orice acțiuni care au ur-

mat. Dacă schimbul de informații are loc fără o astfel de autorizare – pe teren, de pildă, sau în circumstanțe critice – trebuie să se dea explicații clare, în scris, cât mai curând posibil.

Serviciile de informații trebuie să integreze aceste principii în programele lor de instruire și să le comunice organismelor de supraveghere. Totodată, principiile trebuie făcute publice, cu condiția să nu creeze probleme de confidențialitate în materie de securitate națională. Dacă un serviciu de informații nu reușește să dezvolte astfel de principii, organismul care îl supraveghează trebuie să formuleze principii similare și să le aplice în activitatea de supraveghere.

Promovarea unei abordări documentate a schimbului de informații în cadrul unui serviciu de informații

Serviciile de informații trebuie să dețină baze de date care să urmărească antecedentele în materia drepturilor omului în țările cu care fac schimb de informații. Aceste baze de date trebuie:

- să cuprindă o gamă largă de informații publice, inclusiv alegații cu privire la încălcări ale drepturilor omului, provenind de la organisme internaționale și regionale de protecție a drepturilor și de la grupuri credibile din societatea civilă.
- să fie alcătuite prin consultare cu departamentele de afaceri externe.
- să fie folosite pentru instruirea personalului din serviciile de informații.
- să fie puse la dispoziția opiniei publice, cu luarea în considerare a cerințelor de confidențialitate în materie de securitate națională.

Organismele de supraveghere trebuie să aibă acces la aceste baze de date pe care trebuie să le verifice și, dacă este necesar, să le completeze și actualizeze. Dacă un serviciu de informații nu reușește să creeze o astfel de bază de date, organismul care îl supraveghează trebuie să o facă.

Încheierea unor acorduri internaționale pentru schimbul de informații

Serviciile de informații trebuie să încheie acorduri scrise pentru reglementarea schimbului de informații cu parteneri din străinătate. Acordurile trebuie să specifice obligațiile atât ale furnizorilor, cât și ale beneficiarilor de informații în ceea ce priveşte respectarea drepturilor omului. În același timp, trebuie să includă clauze standard care permit ca informațiile primite să fie puse la dispoziția organismului principal de supraveghere a serviciului respectiv și, când este posibil, a organismelor de supraveghere corelate, care acceptă aceleași protocoale de confidențialitate. La conceperea unor astfel de acor-

duri, serviciul de informații trebuie să obțină atât avizul juridic, cât și un aviz de politică externă.

Organismele de supraveghere trebuie să primească copii ale tuturor acordurilor de acest gen în momentul încheierii lor sau atunci când sunt revizuite. Organismului de supraveghere ar trebui să-i revină obligația de a verifica fiecare acord și, când e posibil, de a întreprinde controale aleatorii pentru a stabili măsura în care sunt respectate condițiile acordului. Asemenea controale pot permite să se determine dacă este necesară revizuirea acordului în baza practicii anterioare.

Raportarea și rezolvarea cazurilor de încălcare a avertismentelor atașate informațiilor furnizate

Acordurile privind schimbul de informații trebuie să includă proceduri specifice pentru raportarea de către furnizor a cazurilor de încălcare a avertismentelor pe care le-a atașat informațiilor transmise, precum și pentru rezolvarea disputelor generate de încălcarea avertismentelor. Dacă o agenție furnizoare află despre o astfel de încălcare, ea trebuie să transmită o obiecție formală agenției care a primit informațiile. De asemenea, agenția furnizoare trebuie să folosească prilejul ca pe o oportunitate de a reconsidera acordul în baza căruia s-a făcut schimbul de informații și, posibil, de a face modificări. O astfel de procedură ar putea fi întrebuințată și pentru a corecta sau actualiza informațiile și pentru a propune modificări ale unor avertismente în cazuri specifice sau în timp.

În eventualitatea încălcării unui avertisment (sau chiar a suspectării unei încălcări), serviciile de informații trebuie să înștiințeze organismele care le supraveghează. O asemenea notificare trebuie să includă consemnarea tuturor acțiunilor de remediere pe care serviciul le-a întreprins sau propune să le întreprindă. Organismul de supraveghere trebuie să verifice și să-și exprime punctul de vedere cu privire la toate acțiunile de remediere și, totodată, să abordeze chestiunea generală a modului în care această încălcare ar trebui să influențeze viitoarele schimburi de informații cu partenerul în culpă.

Raportarea și rezolvarea cazurilor de utilizare ilegală a informațiilor care au făcut obiectul schimbului

Serviciile de informații trebuie să înștiințeze organismele care le supraveghează atunci când află (sau chiar suspectează) că informațiile care au făcut obiectul schimbului au fost obținute ilegal sau au fost folosite ori pot fi folosite ilegal, îndeosebi în situația încălcării drepturilor omului. O astfel de notificare trebuie să includă consemnarea tuturor acțiunilor de remediere pe care serviciul le-a întreprins sau propune să le întreprindă. Organismul de supraveghere

trebuie să verifice și să comenteze toate acțiunile de remediere și, totodată, să abordeze chestiunea generală a modului în care această ilegalitate ar trebui să influențeze viitoarele schimburi de informații cu partenerul în culpă.

Încheierea unor acorduri privind schimbul de informații în plan intern

Serviciile de informații trebuie să încheie acorduri scrise prin care să reglementeze schimbul de informații cu partenerii din ţară. Astfel de acorduri trebuie:

- să conțină o autorizare legală precisă.
- să se refere la avertismente și la respectarea drepturilor omului.
- să prevadă piste precise de control (inclusiv evidențe permanente ale tuturor informațiilor furnizate și primite și autorizări scrise atât pentru agențiile care transmit, cât și pentru agențiile care primesc informații).
- să precizeze modul în care schimbul de informații pe plan intern va fi verificat de către organismele competente de supraveghere.

La elaborarea acestor acorduri, serviciul de informații trebuie să obțină un aviz juridic, îndeosebi în privința vieții private și a altor restricții legale referitoare la schimbul de informații. În același timp, avizul juridic trebuie să vizeze și măsura în care jurisdicția organismului de supraveghere a agenției este suficientă pentru verificarea practicilor acesteia privind schimbul de informații.

În abordarea chestiunilor legate de responsabilitate, este necesar ca aceste acorduri să prevadă și să rezolve problemele create de faptul că agențiile care transmit și cele care primesc informații pot fi supuse unor regimuri diferite de supraveghere. Ori de câte ori e posibil, trebuie să se acorde organismelor de supraveghere accesul la toate informațiile de care au nevoie pentru o verificare efectivă a practicilor referitoare la schimbul de informații. Ceea ce poate impune extinderea autorizării legale acordate organismelor interne de supraveghere, pentru a le da posibilitatea să efectueze verificări în comun și să schimbe între ele informații. Totodată, poate impune organismelor de supraveghere să se supună unor măsuri de securitate și secretizare mai stricte decât cele aflate în practica lor obișnuită.

INSTRUMENTUL **8**

Supravegherea financiară a serviciilor de informații

Aidan Wills



8

Supravegherea financiară a serviciilor de informații

Aidan Wills [1]

1. INTRODUCERE

În țările democratice, parlamentele alocă fonduri din trezorerie agențiilor publice, astfel încât acestea să-și poată îndeplini funcțiile și mandatele atribuite prin lege. Ulterior, parlamentele, împreună cu celelalte organisme de supraveghere, monitorizează modul în care sunt cheltuite aceste fonduri pentru a se asigura că utilizarea lor este atât legală, cât și eficientă. Toate agențiile publice, inclusiv serviciile de informații, trebuie să se supună unui astfel de proces.

Acest instrument face o prezentare generală comparativă a modului în care regimurile democratice supraveghează finanțele serviciilor de informații, începând cu alcătuirea bugetelor și mergând până la verificarea *ex post* a cheltuielilor. Obiectivul său este de a evidenția bunele practici. Este compus din următoarele șase secțiuni:

- *Importanța supravegherii financiare a serviciilor de informații* – o explicație a motivului pentru care supravegherea externă este importantă.
- *Bugetele în domeniul intelligence* – o prezentare generală a diferitelor abordări în bugetarea serviciilor de informații.

[1] Acest instrument are la bază lucrările și intervențiile scrise prezentate în cadrul unui atelier DCAF pe tema supravegherii financiare a serviciilor de informații. Printre participanți s-au numărat oficiali de rang înalt din instituții supreme de audit, un reprezentant al unui parlament național, foști oficiali din domeniul intelligence și cadre universitare dintr-o serie de țări. Toate lucrările au fost neoficiale și, prin urmare, nu au fost citate direct. Participanții au oferit, de asemenea, opinii utile privind una dintre versiunile instrumentului de față. Autorul își exprimă recunoștința față de toți membrii acestui grup și aduce totodată mulțumiri colegilor săi din DCAF, Hans Born, Benjamin S. Buckland și Gabriel Geisler Mesevage pentru valoroasele lor comentarii pe marginea unor versiuni mai vechi.

- *Controalele financiare și mecanismele de auditare interne* – o prezentare generală a controalelor și mecanismelor care sporesc eficacitatea supravegherii externe.
- *Supravegherea parlamentară* – o discuție despre rolul parlamentelor în stabilirea bugetelor serviciilor de informații, în supravegherea executării lor și în verificarea cheltuielilor făcute de servicii din punct de vedere al legalității și eficacității.
- *Instituțiile supreme de audit* – o discuție despre rolul instituțiilor supreme de audit (SAI) în auditarea finanțelor serviciilor de informații.
- *Recomandări* – o compilație de bune practici referitoare la supravegherea financiară a serviciilor de informații.

Din rațiuni de spațiu, acest instrument nu abordează rolurile pe care le au executivul, inspectorii generali, procurorii și puterea judecătorească în supravegherea financiară a serviciilor de informații.

Acest instrument utilizează o definiție extinsă a „supravegherii financiare” pentru a include funcții ce pot fi caracterizate și ca exerciții de „control” (a se vedea Born și Geisler Mesevage – Instrumentul 1) și care pot avea loc înainte, pe parcursul și după încheierea activităților financiare supuse supravegherii.

2. IMPORTANȚA SUPRAVEGHERII FINANCIARE A SERVICIILOR DE INFORMAȚII

Există patru motive principale pentru care supravegherea externă a finanțelor serviciilor de informații este importantă:

- Principiile guvernanței democratice impun ca alocarea și utilizarea fondurilor publice să fie verificate îndeaproape.
- Evidenţele financiare pot oferi o imagine relevantă despre conduita și performanțele serviciilor de informații.
- Caracterul secret al activității serviciilor de informații limitează capacitatea opiniei publice de a examina domeniul respectiv.
- Natura muncii de informaţii generează o diversitate de riscuri financiare, inclusiv riscul utilizării incorecte a fondurilor publice.

2.1 GUVERNANȚA DEMOCRATICĂ ȘI UTILIZAREA BANULUI PUBLIC

Un principiu universal acceptat al guvernanței democratice este acela că alocarea fondurilor publice trebuie să fie aprobată de reprezentanții aleși ai poporului – adică de parlament –, fiindcă banii alocați aparțin acestuia. Parlamentele își utilizează competențele bugetare în scopul definirii politicilor și

priorităților care trebuie să stea la baza activităţii entităţilor guvernamentale, astfel încât acestea să reflecte voința populară. La fel de importantă este doctrina potrivit căreia cheltuielile publice trebuie supuse unei verificări *ex post* de către parlament, precum și de către organisme independente ce raportează parlamentului (așa cum sunt SAI). Scopul verificării *ex post* este de a asigura, printre altele, că:

- Fondurile publice au fost întrebuințate în scopurile pentru care au fost alocate de la bun început.
- Cheltuielile respectă legislația aplicabilă (inclusiv legile privind gestionarea fondurilor publice, achizițiile publice, combaterea corupției și legile care reglementează activitățile entității vizate, de exemplu un serviciu de informații).
- Cheltuielile au fost compatibile cu politicile de guvernare.
- Raportul cost-eficacitate a fost bun, permițând realizarea obiectivelor într-o manieră eficace.

Deși aceste principii se aplică, în egală măsură, tuturor agențiilor guvernamentale, inclusiv serviciilor de informații, unele țări exclud explicit serviciile de informații din sfera de acțiune a anumitor legi ce reglementează cheltuirea fondurilor publice. Un exemplu este acela al SUA în ceea ce privește Agenția Centrală de Informații (CIA).[2] În asemenea situații, o verificare atentă este deosebit de importantă.

2.2 EVIDENȚELE FINANCIARE CA INDICATORI DE CONDUITĂ ȘI PERFORMANȚĂ

Finanțele unei agenții publice oferă, de obicei, numeroase informații despre activitățile și performanțele acesteia. Se întâmplă foarte rar ca o agenție să ducă la îndeplinire o sarcină fără a cheltui bani. Prin urmare, evidențele ei financiare vor conține adesea indicii privind activități ascunse, dintre care unele pot fi ilegale. În cazul serviciilor de informații, activitățile ilegale, precum folosirea unor facilități secrete de detenție și finanțarea sub acoperire a unor partide politice autohtone, pot fi descoperite în evidențele financiare ale serviciilor respective. În mod similar, un buget neobișnuit de mare alocat unui departament poate indica performanțe slabe din partea acestuia. Astfel, prin exami-

[2] „Valoare pentru bani” se referă la economicitatea, eficiența și eficacitatea cu care o organizație își folosește resursele în îndeplinirea responsabilităților sale; a se vedea „Performance Audit” [„Auditul performanţei”], în *International Organization of Supreme Audit Institutions, Financial Audit Guideline – Glossary of Terms to the INTOSAI Financial Audit Guidelines.*

narea evidențelor financiare ale unui serviciu, organismele de supraveghere au posibilitatea de a identifica aspecte din munca acelui serviciu, care pot impune o verificare mai aprofundată.

2.3 SECRETIZAREA ȘI LIMITAREA EXAMINĂRII PUBLICE

Dat fiind că munca de informaţii necesită un nivel neobișnuit de mare de secretizare, finanțele serviciilor de informații nu sunt dezvăluite public în aceeași măsură cu cele ale altor agenții guvernamentale. Problema secretizării în zona furnizorilor de bunuri și servicii [3] se complică din cauza faptului că serviciile de informații sunt excluse din sfera de acțiune a majorității legilor ce reglementează accesul public la informațiile deținute de stat, ceea ce limitează volumul de informații pe care le pot obține mass-media și alte organizații ale societății civile. Date fiind aceste limitări impuse examinării publice, e deosebit de important ca organismele de supraveghere externe, care au acces la informații confidențiale, să verifice cu atenție finanțele serviciilor de informații.

2.4 GESTIONAREA RISCULUI FINANCIAR ÎN ACTIVITATEA SERVICIILOR DE INFORMAȚII

Aspectele particulare ale muncii de informaţii creează un risc sporit de utilizare ineficientă sau incorectă a fondurilor publice. Multe dintre aceste aspecte fac din supravegherea serviciilor de informații o misiune foarte dificilă.

2.4.1 Rezultate incerte

Serviciile de informații culeg informații pentru a-i ajuta pe decidenții politici să protejeze securitatea națională. Pentru îndeplinirea acestei funcții, serviciile cheltuiesc bani; însă nu pot fi niciodată sigure că banii cheltuiți vor aduce informațiile căutate. De pildă, un serviciu poate cheltui o mare sumă de bani pentru recrutarea unui informator străin doar ca să descopere că acel informator dispune de prea puține informații de valoare. Cu toate că astfel de riscuri sunt inerente muncii de informaţii, controalele interne și supravegherea externă le pot gestiona, reducând la minimum risipa de fonduri publice.

2.4.2 Beneficii insesizabile

Deși costurile financiare ale unei operațiuni de informaţii pot fi de cele mai multe ori cunoscute, beneficiile pe care le aduc sunt adesea insesizabile. După

[3] SUA, Central Intelligence Agency; appropriations; expenditures [Agenția Centrală de Informații; alocări; cheltuieli], U.S. Code 50 §403j (disponibil la adresa http://us-code.vlex.com/vid/central-intelligence-agency-expenditures-19266900).

cum a remarcat Auditorul General al Canadei, „Rezultatele – și îndeosebi efectele finale – ale operațiunilor de culegere, evaluare și raportare a informațiilor sunt, în mod inerent, dificil de măsurat.” [4] Ceea ce e adevărat, în special, atunci când obiectivul unei operațiuni este prevenirea producerii unui eveniment precum un atac terorist. Numai un organism de supraveghere cu suficient de multe cunoștințe și experiență poate evalua în mod adecvat beneficiile insesizabile ale unei operațiuni de informaţii și poate stabili dacă acestea reflectă un raport corect cost-eficacitate.

2.4.3 Secretizarea și utilizarea incorectă a fondurilor publice

Este de înțeles faptul că serviciile de informații sunt preocupate ca informațiile sensibile, precum detaliile operaționale și identitățile surselor, să rămână confidențiale. În consecință, organizează informațiile pe compartimente, limitând cunoașterea lor la un număr cât mai mic de persoane, chiar din rândul angajaților. Totuși, cu cât este mai mic cercul celor care le cunosc, cu atât este mai mare riscul ca fondurile publice să fie folosite incorect. De exemplu, dacă datele privind un informator sunt cunoscute doar de ofițerul de informații care îl coordonează, se ivește oportunitatea ca ofițerii să creeze „agenți fantomă,” inexistenți, în scopul delapidării fondurilor pe care pretind că le plătesc acestora. Chiar atunci când informatorii sunt reali, regulile de secretizare pot facilita păstrarea de către ofițerii de informații a sumelor destinate informatorilor fără a risca prea mult să fie descoperiți.

2.4.4 Conflicte de interese

Uneori, ca parte a muncii lor, ofițerii de informații plătesc, în secret, anumite persoane în schimbul furnizării de informații sau servicii, cum ar fi folosirea unei case din care să efectueze activități de urmărire. Adeseori, deciziile privind persoana căreia trebuie să i se plătească și suma care trebuie plătită sunt, în mare măsură, la latitudinea ofițerului (și poate a unui supervizor). Ceea ce creează un potențial conflict de interese, fiindcă există probabilitatea ca deciziile ofițerilor să se bazeze nu numai pe meritele celor care furnizează informațiile și/sau serviciile, ci și pe legături personale și, în special, dată fiind natura confidențială a tranzacțiilor, pe gradul de încredere a ofițerului în respectivul furnizor. Drept rezultat, unii ofițeri pot angaja anumite persoane pentru simplul motiv că le cunosc. De asemenea, ei le pot plăti sume excesive,

[4] Pentru exemple ale unor astfel de excepții, a se vedea Marea Britanie, The Defence and Security Public Contracts Regulations 2011, No. 1848 [Reglementări pentru contractele publice în domeniul apărării și securității, 2011, Nr. 1848], Secțiunea 7 (disponibil la http://www.legislation.gov.uk/uksi/2011/1848/made).

fiindcă respectivii furnizori le sunt apropiați. În unele situații, e posibil chiar ca ofițerii să ia mită (a se vedea Caseta 1).

Caseta 1: Cazul lui Kyle Foggo

Kyle Foggo a lucrat la un moment dat ca ofițer superior de informații în cadrul CIA. Printre responsabilitățile sale se număra achiziționarea de bunuri și servicii pentru operațiuni foarte sensibile, inclusiv construirea unor facilități secrete de detenție în străinătate. În vederea achiziționării de materiale pentru unele dintre facilitățile menționate, Foggo a aranjat pentru CIA un contract cu o companie care avea legături cu unul dintre prietenii săi apropiați. Ulterior, procurorii au stabilit că Foggo a direcționat mai multe contracte către această companie, plătind prețuri exagerate pentru bunurile și serviciile furnizate. În schimb, Foggo a primit diverse favoruri, inclusiv vacanțe scumpe și promisiuni de angajare în viitor. Ascunzând relația respectivă față de colegi, Foggo a căutat să justifice folosirea acestei companii susținând că trebuia să achiziționeze bunuri și servicii de la un furnizor în care putea să aibă încredere și că a dorit, totodată, să evite procedura birocratică standard de achiziționare. În final, Foggo a recunoscut acuzația de corupție și a executat o pedeapsă cu închisoarea.[5]

2.4.5 Riscuri asociate bunurilor cu folosință limitată și veniturilor

Serviciile de informații achiziționează un număr considerabil de bunuri cu folosință limitată, ca parte a operațiunilor lor. De pildă, pot cumpăra mașini costisitoare sau folosi hoteluri scumpe pentru a permite unui agent să se apropie de o țintă înstărită pe parcursul unei operațiuni. Ofițerii de informații pot încerca să profite de asemenea bunuri valoroase, odată ce nu mai sunt necesare, prin păstrarea lor pentru uzul personal, prin transferarea lor unor cunoștințe sau prin vânzarea lor și păstrarea sumei respective. Faptul că bunurile respective au fost procurate în secret mărește un astfel de risc. În mod asemănător, unele servicii de informații înființează companii „de fațadă” ca să asigure un paravan pentru activitățile sub acoperire. Unele dintre aceste companii pot genera venituri, creând riscul ca ofițerii implicați să le rețină ilegal pentru ei înșiși. Din cauza unor asemenea riscuri, organismele de supraveghere trebuie să monitorizeze nu numai cheltuielile serviciilor de informații, dar și bunurile și veniturile lor.

5 Auditorul General din Canada, *Report of the Auditor General of Canada* (1996) [*Raportul Auditorului General din Canada* (1996)], Capitolul 27 – „The Canadian Intelligence Community – Control and Accountability” [„Comunitatea de informații din Canada – Control și responsabilitate”], Secțiunea 27.107 (disponibil la http://www.oag-bvg.gc.ca/internet/English/parl_oag_199611_27_e_5058.html).

2.4.6 Utilizarea serviciilor de informații în scopuri politice

Întrebuințarea incorectă a fondurilor de care dispun serviciile de informații se poate extinde la membrii executivului care răspund de activitatea respectivelor servicii. Oficialii din această categorie au folosit uneori resursele unui serviciu în scopuri politice ilegale, implicând cheltuieli din fonduri publice. Așadar, e necesar ca organismele de supraveghere să-și concentreze atenția nu numai asupra conduitei ofițerilor din servicii, ci și asupra interacțiunilor dintre aceștia și oficialii din executiv.

3. BUGETELE ÎN DOMENIUL INTELLIGENCE

Un *buget* este un document defalcat pe elemente, care detaliază veniturile și cheltuielile planificate pentru o perioadă imediat următoare, de regulă un an fiscal. Ca atare, el reprezintă un instrument cheie pentru conducerea și controlarea activității unei agenții publice, dat fiind că agențiile au nevoie de finanțare ca să funcționeze. În țările democratice, bugetele sunt adoptate, în mod normal, de către parlamente, ca elemente de legislație.

În unele țări, serviciile de informații sunt autonome din punct de vedere organizațional și au propriile lor bugete. În alte țări, ele funcționează în cadrul ministerelor – ca în situația ministerului francez al afacerilor interne, care include în structura sa serviciul de informații interne (la Direction Centrale du Renseignement Intérieur). În acest ultim exemplu, serviciile de informații nu au bugete proprii. În schimb, sunt finanțate din bugetul ministerului de care aparțin. Așa că termenul de *buget în domeniul intelligence* poate duce la confuzii, făcând uneori referire la bugetul unui singur serviciu și alteori, la bugetul mai multor servicii din cadrul unui singur minister. Termenul se poate referi și la sume agregate, destinate unei întregi comunități de informații, care implică mai multe ministere. Trebuie să se remarce, de asemenea, că, în unele țări, nu toate cheltuielile legate de serviciile de informații sunt incluse în bugetele acestora. Mai ales cheltuielile pentru pensii și bunuri precum rechizitele pot fi incluse în alte capitole ale bugetului de stat. Ceea ce poate face dificilă calcularea bugetului general pentru serviciile de informații.

Situația organizațională a unui serviciu este importantă datorită implicațiilor pe care le are asupra activității de verificare a bugetului său. Ca regulă generală, cei care efectuează o supraveghere din exterior pot verifica mai direct și mai amănunțit finanțele serviciilor de informații înființate ca agenții autonome decât atunci când agențiile funcționează în cadrul unui minister. Și asta, deoarece finanțele unui serviciu autonom nu se întrepătrund cu cele ale altor departamente ministeriale.

Bugetele agențiilor guvernamentale, indiferent dacă lucrează în domeniul informațiilor sau nu, trebuie să fie „cuprinzătoare.” Banca Mondială întrebuințează acest termen în sensul că bugetele „trebuie să înglobeze toate operațiunile fiscale.”[6] Cu alte cuvinte, bugetul unei agenții guvernamentale trebuie să includă întreaga activitate financiară aferentă acelei agenții.[7] Serviciile de informații, în mod special, trebuie să respecte această cerință, fiindcă unele dintre ele au antecedente de încasare a banilor și de cheltuire a lor în activități neautorizate prin lege. Un exemplu ar fi utilizarea de către CIA a veniturilor obținute prin vânzarea de arme către Iran pentru a susține financiar contrarevoluționarii („contras”) din Nicaragua la mijlocul anilor ‘80.

3.1 CICLUL BUGETAR

Termenul de *ciclu bugetar* se referă la procesul complet prin care banii sunt solicitați, alocați și cheltuiți (inclusiv verificarea *ex post* a acestei cheltuiri). Există patru etape principale în ciclul bugetar:

- elaborarea, etapă în care ministerele și departamentele guvernamentale responsabile și agențiile determină veniturile și cheltuielile planificate;
- examinarea și aprobarea, etapă în care parlamentul amendează și adoptă bugetul;
- execuția, etapă în care agenția pune în practică planul detaliat în buget;
- verificarea *ex post*, etapă în care organismele de supraveghere examinează modul în care agenția a utilizat banii; controlul poate fi urmat de un vot parlamentar pentru „descărcarea de gestiune” a guvernului

---

6 Pentru mai multe informații, a se vedea David Johnston și Mark Mazzetti, „A Window Into C.I.A.’s Embrace of Secret Jails” [„O explicaţie a utilizării de către CIA a închisorilor secrete”], în *New York Times*, 12 August 2009; David Johnston, „Ex-C.I.A. Official Admits Corruption” [„Fost oficial CIA recunoaște corupția”], în *New York Times*, 29 septembrie 2008; Matthew Barakat, „Feds: Misconduct by CIA’s Foggo spanned decades” [„Federalii: conduita incorectă a agentului CIA Foggo de-a lungul deceniilor”], în *Associated Press*, 25 februarie 2009; și *U.S. v. Foggo and Wilkes* [*Statele Unite versus Foggo și Wilkes*], Tribunalul Districtual SUA din California de Sud, Act de acuzare al Marelui Juriu, iunie 2005.

7 Banca Mondială, *Public Expenditure Management Handbook* [*Manual de gestiune a cheltuielilor publice*] (Washington: The World Bank, 1998), „Code of Practices on Fiscal Transparency” [„Codul de practici privind transparența fiscală”], Anexa J.

privind execuția bugetară (aprobarea și certificarea bilanțurilor contabile) pentru un anumit an.[8]

Deși bugetele serviciilor de informații sunt elaborate aproape în aceeași manieră ca bugetele celorlalte departamente și agenții guvernamentale, procedurile de examinare și aprobare, de execuție și de verificare *ex post* (prezentate în secțiunile 5-6 ale instrumentului de față) sunt diferite.

3.2 ABORDĂRI ALE BUGETĂRII

Modul tradițional de bugetare utilizează metoda defalcării pe elemente, alocând sume specifice (intrări) pentru costuri sau capitole de buget, fără a corela aceste intrări cu obiective de politică sau ieșiri. În opoziție cu această abordare bazată pe intrări, multe țări (precum Franța) folosesc în prezent o metodă de bugetare pe baza „performanțelor” sau a „rezultatelor,” care corelează alocarea de fonduri cu obiective de politică și, în final, cu rezultatele dorite.[9] Modul de abordare a bugetării are implicații importante pentru supravegherea *ex post*. Deoarece bugetarea pe bază de rezultate stabilește o legătură între intrări și ieșiri, este mai ușor să se evalueze ulterior modul de execuție a unui buget, inclusiv factori precum eficiența și raportul cost-eficacitate. Prin contrast, bugetarea pe baza intrărilor nu asigură un cadru pentru evaluarea executării bugetului.

3.3 PUBLICAREA BUGETELOR DIN DOMENIUL INTELLIGENCE

După știința autorului, nu există niciun guvern care să facă publice în întregime bugetele serviciilor sale de informații. În majoritatea țărilor, detaliile clasificate ale bugetelor nu sunt accesibile nici membrilor publicului larg, nici parlamentarilor care nu fac parte din comisiile autorizate să acceseze informații clasificate în materie.

---

8 Todor Tagarev (ed.), *Building Transparency and Reducing Corruption in Defence: A Compendium of Best Practices* [*Creșterea transparenței și reducerea corupției în domeniul apărării: compendiu al celor mai bune practici*] (Geneva: NATO/DCAF, 2010), p. 64. Ca exemplu din legislația națională, a se vedea Africa de Sud, Public Finance Management Act No. 1 of 1999 [Legea nr. 1 din 1999 privind gestiunea finanțelor publice], Secțiunea 38(2).

9 Pentru o discuție mai detaliată asupra diferitelor abordări ale modului de alocare a bugetului, a se vedea Banca Mondială, *Public Expenditure Management Handbook* [*Manual de gestiune a cheltuielilor publice*], pp. 12–16; Tagarev, *Building Transparency and Reducing Corruption in Defence*, p. 59; și Organizația pentru Cooperare și Dezvoltare Economică (OCDE), „Performance Budgeting: A User’s Guide” [„Bugetarea pe bază de performanțe: ghid pentru utilizatori”], Document orientativ (martie 2008).

Secretul care înconjoară bugetele din domeniul intelligence este motivat de temerea serviciilor de informații că publicarea detaliilor bugetare va fi în avantajul adversarilor lor. Totuşi, o astfel de îngrijorare ar putea fi întemeiată doar dacă informațiile difuzate public ar conține detalii referitoare la anumite ținte, metode ori surse de informații. În majoritatea cazurilor, pot fi făcute publice mult mai multe informații decât se întâmplă în prezent, fără a implica riscuri la adresa securității naționale și sporind, în schimb, considerabil gradul de transparență.

În general, țările democratice aleg între trei tipuri de abordare pentru asigurarea accesului public la bugetele din domeniul intelligence. Unele țări (precum Marea Britanie [10]) fac publică doar suma totală, alocată întregii comunități naționale de informații. Altele (ca Germania) fac publică suma totală individuală pentru fiecare serviciu de informații. Evident, nici una din aceste abordări nu face publice legăturile dintre resursele alocate și obiectivele specifice ale politicilor respectivelor servicii de informații, care ar putea fi utile în dezbaterea publică. Cel de-al treilea tip de abordare (folosit în Australia și Franța, de exemplu) este să facă publice sume precise, alocate anumitor scopuri. De pildă, bugetul anual făcut public pentru Direction Générale de la Securité Extérieure (DGSE), serviciul francez de informații externe, enumeră separat cheltuielile autorizate pentru personal, costuri operaționale și investiții; de asemenea, este publică suma totală destinată activităților speciale operaționale (*les fonds spéciaux*).

Totodată, guvernele care folosesc metoda bugetării pe baza performanțelor (cum o fac și Australia și Franța) pot face publice obiective ale politicilor și rezultatele dorite în așa fel, încât cetățenii să poată vedea singuri legăturile.[11] De exemplu, versiunea publică a bugetului DGSE pe anul 2010 a stabilit drept obiectiv principal al politicilor „ameliorarea capacității DGSE de a culege și analiza informațiile,” menționând recrutarea planificată a unui număr suplimentar de 690 de angajați între 2009 și 2015 ca mijloc de atingere a acestui obiectiv.[12]

Asigurarea accesului public la cât mai multe informații bugetare posibil – ceea ce reușește mai bine cea de-a treia abordare prin comparație cu primele

---

[10] Bugetul unic al domeniului intelligence din Marea Britanie reunește bugetele celor trei servicii civile de informații.

[11] Pentru o discuție mai detaliată, a se vedea Nicolas Masson și Lena Andersson, *Guidebook: Strengthening Financial Oversight in the Security Sector* [*Ghid: întărirea supravegherii financiare în sectorul de securitate*] (Geneva: DCAF, 2012).

[12] Franța, Mission Ministérielle Projets Annuels de Performances, „Annexe au projet de loi de finances pour Défense” [Misiunea ministerială Proiecte anuale de performanță, „Anexă la proiectul legii finanțelor pentru apărare”] (2010), pp. 36–37.

două – este benefică societății din mai multe motive. În primul rând, se respectă dreptul populației de a cunoaște cum sunt cheltuiți banii. În al doilea rând, crește transparența, ceea ce permite simplilor membri de parlament (adică celor care nu fac parte din comisiile autorizate să acceseze informații clasificate din domeniu), mass-mediei și chiar unor cetățeni oarecare să aibă o participare semnificativă la dezbaterea publică privind finanţarea, politicile şi priorităţile serviciilor de informații. O dezbatere publică serioasă obligă guvernele să-și justifice prioritățile în privința cheltuielilor, ceea ce, în final, poate stimula o utilizare mai eficientă a fondurilor publice. În fine, o dezbatere deschisă mărește încrederea publică în serviciile de informații, spulberând miturile în legătură cu scopurile cheltuielilor din acest domeniu și chiar ducând, în timp, la creșterea fondurilor alocate serviciilor de informații.

Decizia privind cât de multe informații bugetare pot fi făcute publice nu trebuie lăsată doar la latitudinea executivului. Parlamentele trebuie să reglementeze, cu ajutorul legislației, care informații financiare pot fi păstrate secrete și care trebuie dezvăluite. Indiferent de volumul informațiilor financiare care au devenit publice, este esențial să se acorde comisiilor parlamentare, implicate în verificarea, amendarea și/sau aprobarea bugetelor din domeniul intelligence, acces la toate informațiile relevante, inclusiv la secțiunile clasificate ale bugetului (a se vedea Secțiunea 5.1).[13]

4. CONTROALELE FINANCIARE ȘI MECANISMELE DE AUDITARE INTERNE

Deși acest instrument se axează pe rolul jucat de organismele externe de supraveghere în monitorizarea finanțelor serviciilor de informații, prezentarea ar fi incompletă fără a discuta întrucâtva despre controalele financiare interne care există în cadrul serviciilor de informații. În absența unor astfel de mecanisme, supravegherea externă nu ar putea fi eficace.

4.1 CONTABILITATEA

În mod normal, legislația impune tuturor agențiilor publice, inclusiv serviciilor de informații, să desemneze un contabil a cărui responsabilitate este să se asigure că agenția păstrează evidenţe financiare ordonate și exacte și că respectă toate reglementările aplicabile (a se vedea Caseta 2). Adesea, respectivele atribuții de natură contabilă revin directorului agenției, care e sprijinit în această misiune de un departament financiar ce efectuează activitatea curentă

[13] Referitor la importanța decidenților care au acces la toate informațiile bugetare, a se vedea Banca Mondială, *Public expenditure Management Handbook* [*Manual de gestiune a cheltuielilor publice*], pp. 1–2.

de înregistrare și raportare a tuturor tranzacțiilor financiare făcute de agenție. Totodată, departamentele financiare instituie și efectuează controale financiare pentru a se asigura că resursele sunt folosite în mod corespunzător.

Caseta 2: Legislația sud-africană cu privire la contabili

Caseta de față compilează prevederi selectate din „Legea privind gestiunea finanțelor publice" din Africa de Sud, din 1999, care reglementează controalele financiare interne pentru agențiile guvernamentale (inclusiv serviciile de informații). În conformitate cu legea menționată, contabililor le revine o responsabilitate importantă în a se asigura că agențiile lor folosesc practici financiare corecte.

Fiecare agenție a guvernului sud-african trebuie să aibă un contabil care răspunde pentru:

1. asigurarea faptului că agenția menține un sistem eficace, eficient și transparent de gestionare a riscurilor financiare, precum și un sistem intern de auditare, aflat sub controlul unei comisii de audit ce funcționează în conformitate cu reglementările aplicabile.
2. utilizarea eficace, eficientă, economicoasă și transparentă a resurselor agenției.
3. gestionarea activelor și pasivelor agenției, inclusiv protejarea bunurilor agenției.
4. asigurarea faptului că agenția respectă legislația bugetară în materie de cheltuieli.

Legea mai atribuie contabililor sarcina de a preveni și, acolo unde este necesar, de a reacționa la cheltuielile neautorizate, neregulamentare sau excesive ale agenției. Atunci când se descoperă astfel de cheltuieli, contabilul trebuie să raporteze trezoreriei imediat, în scris, detaliile acestora, iar în cazul unor cheltuieli neregulamentare, care implică achiziționarea de bunuri sau servicii, trebuie să se adreseze comisiei de achiziții. În plus, contabilul trebuie să ia măsuri disciplinare adecvate împotriva oricărui oficial care subminează sistemul de gestiune financiară al agenției sau care face (ori permite să se facă) cheltuieli neautorizate, neregulamentare sau excesive.

În ceea ce privește păstrarea evidenței, contabilul trebuie să păstreze evidențe complete și corecte ale operațiunilor financiare ale agenției, în conformitate cu normele și standardele aplicabile.

O contabilitate internă corectă este esențială pentru munca organismelor externe de supraveghere, deoarece, în lipsa ei, SAI și alte organisme de acest gen ar întâmpina dificultăți majore în reconstituirea tranzacțiilor și a activităților asociate. În general, calitatea contabilităţii unui serviciu de informații indică dacă evidențele financiare sunt corecte și reflectă realitatea.

4.2 LINII DIRECTOARE PENTRU GESTIUNEA FINANCIARĂ

La fel ca toate agențiile guvernamentale, serviciile de informații își formalizează procedurile de gestiune financiară și evidență contabilă într-un set de linii directoare în formă scrisă. Emise în mod normal de directorul serviciului sau de executiv și, apoi, analizate de un organism extern de supraveghere, aceste linii directoare devin parte a cadrului normativ cu ajutorul căruia sunt evaluate acțiunile angajaților din serviciul respectiv.

De regulă, liniile directoare pentru gestiunea financiară se referă la următoarele aspecte:

- De către cine și în ce mod sunt autorizate realizarea de venituri și efectuarea de cheltuieli? Prin răspunsul la această întrebare, liniile directoare trebuie să prevadă clar nivelurile de responsabilitate și răspundere pentru tranzacțiile financiare.
- Ce utilizări sunt permise pentru fondurile serviciilor? Răspunsul la această întrebare trebuie să fie în conformitate cu legislația relevantă.
- Cum trebuie să se desfășoare tranzacțiile financiare? Liniile directoare trebuie să recomande, de pildă, dacă agenții trebuie să facă plăți în numerar sau electronice.
- Ce evidențe financiare trebuie păstrate? O evidență corectă e importantă, deoarece stabilește o pistă de audit care va putea fi folosită ulterior. Cu toate acestea, în unele țări, precum SUA, legea permite serviciilor de informații să utilizeze „conturi fără voucher” (cheltuieli justificate exclusiv prin certificarea lor de către un membru al executivului și care nu sunt susținute de un set complet de chitanțe) în legătură cu unele operațiuni sensibile (de exemplu operațiuni în domeniul informațiilor externe).[14]

4.3 RAPORTAREA FINANCIARĂ

În mod normal, legea impune agențiilor publice, inclusiv serviciilor de informații, să pregătească rapoarte anuale detaliate privind tranzacțiile lor fi-

[14] SUA, Oficiul Guvernamental de Conturi (GAO), Central Intelligence Agency: Observations on GAO Access to Information on CIA Programs and Activities [Agenția Centrală de Informații: observații privind accesul GAO la informații despre programele și activitățile CIA], GAO-01-975T (iulie 2001), p. 10; și SUA Central Intelligence Agency; appropriations; expenditures [Agenția Centrală de Informații; alocări; cheltuieli], U.S. Code 50 §403j.

nanciare.[15] Fără astfel de rapoarte, organismele externe de supraveghere nu ar putea verifica finanțele și activitățile serviciilor.

De obicei, serviciile de informații prezintă aceste rapoarte executivului, instituțiilor SAI și parlamentului. Totuși, ca și în cazul bugetelor, rapoartele pot varia din punct de vedere al volumului de detalii oferite.

Tot așa cum executivului ar trebui să nu i se acorde puterea de a determina în mod unilateral care informații bugetare pot fi făcute publice și care nu, în același mod ar trebui să nu i se acorde nici puterea de a stabili singur care informații pot fi incluse în rapoartele financiare și care anume pot rămâne secrete. În schimb, parlamentul ar trebui să stabilească prin legislație criterii detaliate, care să reglementeze categoriile de informații financiare ce trebuie făcute publice și cele care pot rămâne confidențiale (a se vedea Caseta 3).

Caseta 3: Raportarea financiară conform legislației din Noua Zeelandă

Această casetă selectează prevederi din „Legea finanțelor publice" din 1984 și din „Legea privind Serviciul de Informații de Securitate" din 1969, care, luate împreună, reglementează modul în care serviciile de informații din Noua Zeelandă își pregătesc rapoartele financiare. În același timp, se face o comparație între cerințele impuse serviciilor de informații și cele impuse altor organisme publice.

În cel mai scurt timp posibil după încheierea fiecărui an fiscal, organismele publice din Noua Zeelandă (inclusiv serviciile de informații) trebuie să pregătească rapoarte financiare care acoperă anul fiscal anterior și să le prezinte ministrului responsabil. Rapoartele trebuie să cuprindă date financiare complete, precum și informații referitoare la operațiunile agenției și o situație a performanțelor acesteia. În general, rapoartele trebuie să ofere îndeajuns de multe informații pentru a permite o evaluare documentată a rezultatelor obținute în decursul anului fiscal anterior – în special cu privire la obiectivele, indicatorii și normele stabilite pentru respectiva agenție la începutul anului.

În cazul majorităţii organismelor publice, legislația impune ministrului responsabil ca, odată ce a primit raportul, să îl prezinte parlamentului, după care, să îl publice în cel mai scurt timp. Însă în cazul rapoartelor primite de la serviciile de informații, procedurile diferă. În loc să prezinte întregul raport în plenul parlamentului, ministrul responsabil îl prezintă doar Comisiei pentru informații și securitate, ai cărei membri sunt autorizați să consulte informații clasificate. Pentru plenul parlamentului, ministrul pregătește o versiune editată, care trebuie să includă o situație a cheltuielilor totale. Această versiune editată a raportului va fi făcută publică ulterior de ministrul respectiv.

[15] A se vedea, de exemplu, Australia, Financial Management and Accountability Act [Lege privind gestiunea financiară și responsabilitatea], 1997, Secțiunea 49.

Ca și în cazul bugetelor pentru serviciile de informații, Australia și Franța oferă exemple de bune practici în acest sens. Serviciile lor de informații pregătesc rapoarte financiare relativ detaliate, care sunt făcute publice. Rapoartele puse la dispoziția publicului de Organizația Australiană pentru Informații de Securitate (ASIO) conțin subtotaluri pentru categorii de cheltuieli precum cele de personal, aprovizionare (inclusiv bunuri și servicii) și costuri de uzură/amortizare. Rapoartele mai cuprind subtotaluri pentru categorii de venituri, precum venituri din surse proprii, din vânzări de bunuri și venituri de la guvern.[16] Legea franceză impune ca rapoartele financiare ale serviciilor de informații să includă anexe detaliate pentru fiecare misiune a acestora. Astfel de anexe trebuie să includă nu numai datele financiare, ci și o evaluare a obiectivelor aferente politicilor și a rezultatelor dorite, așa cum au fost stabilite la începutul ciclului bugetar.[17]

Din aceleași rațiuni menționate mai sus (a se vedea Secțiunea 3.3) în legătură cu informațiile bugetare, serviciile de informații trebuie să elaboreze versiuni publice cât mai detaliate posibil ale rapoartelor lor financiare, fără a prejudicia caracterul confidențial al muncii lor și fără a pune în pericol securitatea națională.

5. SUPRAVEGHEREA PARLAMENTARĂ

Această secțiune se axează pe rolul jucat de parlament pe parcursul celor trei etape finale ale ciclului bugetar – examinare și aprobare, execuție și verificare *ex post*. Deși munca serviciilor de informații implică chestiuni sensibile, parlamentele trebuie să examineze finanțele acestora în aceeași măsură în care examinează finanțele celorlalte agenții publice. Singura concesie făcută trebuie să fie utilizarea unor mecanisme mai precaute de supraveghere.

Majoritatea activităților de supraveghere parlamentară a serviciilor de informații au loc, inevitabil, cu ușile închise. Cu toate acestea, rămâne la fel de important ca parlamentarii să asigure informarea la zi a populației cu privire la activitatea de supraveghere, prin intermediul unor rapoarte publice și al unor audieri publice (a se vedea Nathan – Instrumentul 3). Transparența promovează încrederea publică în supravegherea parlamentară, dar și în munca serviciilor de informații.

---

[16] Organizația Australiană pentru Informații de Securitate, „Financial Statements” [„Situaţii financiare”], în *Annual Report 2010–11* (Canberra: 2011), pp. 133–151 (disponibil la http://www.asio.gov.au/img/files/Report-to-Parliament-2010-11.pdf).

[17] Franța, Loi organique n°2001–692 du 1 août 2001 relative aux lois de finances (LOLF) [Legea organică nr. 2001-692 din 1 august 2001 privind legile finanțelor (LOLF)], Articolul 54.

5.1 EXAMINAREA ȘI APROBAREA BUGETELOR

În cele mai multe țări democratice, parlamentele examinează, amendează și aprobă bugetele agențiilor, propuse de executiv. Nu există niciun motiv valabil pentru care bugetele serviciilor de informații să fie excluse din acest proces.

În vederea protejării informațiilor clasificate, parlamentele pot înființa mecanisme speciale pentru examinarea secțiunilor clasificate ale bugetului. Însă, indiferent de mecanismele folosite, plenul trebuie să se pronunțe prin vot întotdeauna cu privire la sumele alocate serviciilor de informații, ca parte a procesului de aprobare a bugetului prezentat de guvern. Voturile din plen trebuie să fie o completare la – și nu un substitut pentru – examinarea completă efectuată de o comisie sau, în comun, de mai multe comisii precum: comisia pentru buget, comisia pentru supravegherea serviciilor de informații sau o comisie specială pentru chestiuni confidențiale.[18]

5.1.1 Comisiile pentru buget

Unele parlamente utilizează comisiile standard pentru buget (sau alocații) în scopul examinării finanțelor serviciilor de informații. Comisiile își pot desemna anumiți membri ca raportori, aceștia urmând să răspundă de un anumit serviciu, minister sau de o anumită misiune. Respectivii raportori elaborează, de regulă, rapoarte conținând recomandări pe baza cărora întreaga comisie dezbate, amendează și aprobă bugetele serviciilor.

Comisiile pentru buget sunt, din multe puncte de vedere, bine poziţionate pentru a evalua bugetele serviciilor de informații în contextul mai larg al bugetului pentru întregul executiv. Dar, în absența raportorilor specializați, există probabilitatea ca membrii comisiilor să nu aibă timpul necesar ori expertiza specifică în materie, care să le permită examinarea corespunzătoare a bugetelor serviciilor de informații. Totodată, comisiile pentru buget nu dispun, de regulă, de suficient acces la informațiile clasificate, ceea ce le limitează capacitatea de a examina bugetele serviciilor.

---

18 Pentru o discuție despre modelul italian în care parlamentul votează o sumă globală, lăsând la discreția guvernului alocarea specifică de fonduri, a se vedea Federico Fabbrini și Tomasso Giupponi, „Parliamentary and Specialised Oversight of Security and Intelligence Agencies in Italy” [„Supravegherea parlamentară și specializată a agențiilor de securitate și de informații în Italia”], în *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, Aidan Wills și Mathias Vermeulen (Bruxelles: Parlamentul European, 2011), Anexa A, p. 245.

5.1.2 Comisiile de supraveghere a serviciilor de informații

Comisiile de supraveghere a serviciilor de informații au acces, în mod normal, la informații clasificate care nu sunt disponibile celorlalți parlamentari (a se vedea Farson – Instrumentul 2 și Nathan – Instrumentul 3). De regulă, ele își concentrează atenția asupra verificării *ex post* a activităților derulate de servicii, inclusiv asupra finanțelor acestora. Totuși, în unele țări, responsabilitățile lor se extind și la examinarea și aprobarea bugetului. În Ungaria, Comisia parlamentară pentru securitatea națională examinează și emite un aviz cu privire la bugetele propuse pentru serviciile de informații. Această activitate include examinarea secțiunilor clasificate ale bugetului, care nu sunt puse la dispoziția plenului parlamentului.[19] Procesul mai complex din cadrul Congresului SUA este descris în Caseta 4. În alte țări (de exemplu, în Germania, a se vedea Caseta 5), comisiile de supraveghere a serviciilor de informații au un rol secundar, de emitere a unui aviz pentru alte comisii (cum sunt cele pentru buget sau pentru alocații), care au responsabilitatea principală în examinarea bugetelor.

Comisiile de supraveghere a serviciilor de informații sunt, cu precădere, structuri adecvate pentru examinarea și înțelegerea bugetelor acestor servicii, dat fiind faptul că sunt familiarizate cu activitatea, procedurile și politicile lor. Totuși, eficacitatea examinării la acest nivel depinde de mai mulți factori:

- resursele comisiei, competențele sale de investigare și accesul la informații clasificate;
- măsura în care membrii comisiei au timpul, stafful și expertiza necesare pentru a-și îndeplini responsabilitățile;
- dorința membrilor comisiei de a-și duce la îndeplinire responsabilitățile;
- capacitatea comisiei de a influența procesul bugetar (în special atunci când rolul său este de avizare).

Dacă circumstanțele o cer, comisiile de supraveghere a serviciilor de informații, care au responsabilități bugetare semnificative, pot utiliza competența de aprobare (în colaborare cu alte comisii relevante) pentru a se asigura că bugetele propuse țin seama de recomandările prealabile ale comisiilor cu privire la căile prin care se pot ameliora eficacitatea și eficiența serviciilor și gradul în care acestea respectă legislația.

[19] Ungaria, Act CXXV of 1995 on the National Security Services [Legea CXXV din 1995 privind serviciile de securitate națională], Articolul 14(g).

Caseta 4: Examinarea și aprobarea de către Congres a bugetelor serviciilor de informații din SUA [20]

Procesul prin care Congresul SUA examinează și aprobă bugetele serviciilor de informații implică nu mai puțin de opt comisii și subcomisii și are două aspecte distincte: autorizarea și alocarea.

Autorizarea

Proiectele de lege de autorizare ale Congresului, atunci când sunt semnate de președinte, reglementează activitățile agențiilor guvernamentale, inclusiv bugetele lor. Pentru bugetele serviciilor de informații, procesul de autorizare începe cu propunerile înaintate Congresului de către executiv. Propunerile sunt examinate, în Camera Reprezentanților, de Comisia permanentă pentru informații și Comisia pentru forțele armate, iar la Senat, de Comisia pentru informații și Comisia pentru forțele armate. Aceste comisii pot modifica alocarea sumelor în cadrul bugetelor; totodată, pot interzice anumite activități și pot include noi inițiative. Odată ce comisiile unei Camere au finalizat un proiect de lege de autorizare, se trece la votarea lui de către plen. După aprobarea atât de Cameră, cât și de Senat a proiectelor de lege de autorizare, acestea trec prin procesul de mediere. Proiectul final este aprobat din nou de fiecare Cameră și este transmis președintelui spre semnare.

Fiecare proiect de lege de autorizare în domeniul intelligence are o anexă clasificată, care enumeră pe categorii de activități sumele pe care fiecare serviciu este autorizat să le primească și scopurile cărora le sunt destinate respectivele fonduri. Astfel, proiectele de lege de autorizare (devenite legi după semnare) stabilesc parametrii cheltuielilor din domeniul intelligence. Cu toate acestea, legile de autorizare nu garantează că programele autorizate vor primi într-adevăr fonduri. Decizia finală de acordare a fondurilor e adoptată în cursul procesului de alocare.

---

[20] Richard Best, *The Intelligence Appropriations Process: Issues for Congress* [*Procesul de alocare în domeniul intelligence: probleme în atenția Congresului*] (Washington: Congressional Research Service, 27 octombrie 2011); a se vedea și Richard Best și Elizabeth Bazan, *Intelligence Spending: Public Disclosure Issues* [*Cheltuielile din domeniul intelligence: aspecte ale comunicării publice*] (Washington: Congressional Research Service, 15 februarie, 2007), p. 5; Frederick Kaiser, Walter Oleszeck și Todd Tatelman, *Congressional Oversight Manual, Congressional Research Service* [*Manual privind activitatea Congresului de supraveghere, Serviciul de cercetare al Congresului*] (Washington: Congressional Research Service, iunie 2011), pp. 16–19; Eric Rosenbach și Aki Peritz, *Confrontation or Collaboration? Congress and the Intelligence Community* [*Confruntare sau colaborare? Congresul și comunitatea de informații*] (Cambridge, MA: Harvard, 2009), pp. 24–28; și James Saturno, *The Congressional Budget Process: A Brief Overview* [*Procesul bugetar în Congres: o prezentare succintă*] (Washington: Congressional Research Service, 2004).

Alocarea

Legea de alocare a creditelor bugetare este similară legislației bugetare din alte țări; este instrumentul legislativ prin care se alocă fonduri din trezorerie unei agenții sau unui program. Atât Comisia pentru buget a Camerei, cât și Comisia pentru buget a Senatului au subcomisii pentru apărare cu atribuții în ceea ce privește bugetele aferente cvasi-totalității agențiilor care fac parte din comunitatea de informații din SUA. Pe baza propunerilor primite din partea executivului, aceste subcomisii elaborează proiectele de lege de alocare a creditelor bugetare în domeniul intelligence.

Deși proiectele de lege de alocare trebuie să se conformeze, în general, legislației de autorizare existente, ele pot mări sau reduce fondurile pentru anumite programe din domeniul intelligence. Dacă nu există o astfel de legislație, proiectele de lege de alocare pot include autorizări generale pentru întreaga activitate din acest domeniu.

Ca și în cazul legilor de autorizare, proiectele de lege de alocare a creditelor bugetare trebuie să parcurgă un proces complex de aprobare. Ele trebuie să fie aprobate de subcomisii, după aceea de comisii, în ansamblu, apoi de plenul fiecărei camere, după care ajung la mediere. Proiectul final este aprobat din nou de fiecare Cameră și este transmis președintelui spre semnare.

5.1.3 Comisiile speciale pentru chestiuni confidențiale

Uneori, parlamentele fac uz de un al treilea mecanism, comisia specială pentru chestiuni confidențiale, pentru a examina bugetele serviciilor de informații. Un bun exemplu al unui astfel de mecanism este Comisia pentru chestiuni confidențiale înființată de Bundestag-ul german (a se vedea Caseta 5).

5.2 MONITORIZAREA EXECUȚIEI BUGETELOR

Odată aprobate bugetele agențiilor publice, parlamentele au responsabilitatea de a monitoriza cheltuielile agențiilor pentru a se asigura că execuția bugetelor se face în mod corespunzător. În cazul serviciilor de informații, monitorizarea este efectuată, de obicei, de comisia parlamentară de supraveghere a respectivelor servicii (sau de o comisie specială pentru chestiuni confidențiale) ai cărei membri dispun de acces privilegiat la informații clasificate. În practică, însă, comisiile de supraveghere a serviciilor de informații au tendința să solicite informații financiare doar dacă au apărut alegații referitoare la o conduită incorectă într-un anumit program sau într-o anumită activitate. Și aceasta, fiindcă cei mai mulți parlamentari nu au nici timpul, nici resursele necesare pentru a examina în detaliu un mare volum de informații financiare pe parcursul unui an.

Caseta 5: Comisia pentru chestiuni confidențiale din Bundestag-ul german [21]

Bundestag-ul, camera inferioară a parlamentului german, repartizează chestiunile bugetare care implică cele trei servicii federale de informații unei comisii speciale pe care a înființat-o, Comisia pentru chestiuni confidențiale. Această comisie are aceleași funcții pe care le îndeplinesc Comisia pentru buget și Comisia pentru auditul public din Bundestag în privința altor departamente și agenții publice. Și anume, examinează și poate amenda bugetele propuse de executiv și verifică execuția lor. Caseta de față prezintă funcțiile comisiei privind examinarea și aprobarea bugetului.

Alegerea membrilor comisiei

Comisia pentru chestiuni confidențiale are zece membri; cele zece locuri se alocă proporțional partidelor politice în funcție de reprezentarea fiecărui partid în Bundestag. Cei nominalizați nu au nevoie de certificat de securitate, însă trebuie să fie aleși prin ceea ce se numește „majoritatea cancelarului," adică să fie votați de majoritatea membrilor Bundestag-ului – un indiciu al faptului că se bucură de încrederea parlamentului.

Examinarea și aprobarea bugetelor din domeniul intelligence

Examinarea și aprobarea de către comisie a bugetelor serviciilor de informații se desfășoară după cum urmează:

1. Executivul înaintează comisiei bugetul detaliat al fiecărui serviciu de informații.
2. Comisia se întâlnește cu oficiali din minister și cu membri ai conducerii superioare a serviciilor de informații pentru a discuta despre bugetele propuse.
3. Comisia se consultă cu comisia de supraveghere a serviciilor de informații din Bundestag.
4. Comisia amendează bugetul după cum consideră necesar înainte de a-l retransmite executivului care, de obicei, trebuie să accepte modificările.
5. Președintele comisiei transmite Comisiei pentru buget sumele totale alocate fiecărui serviciu. Apoi, Comisia pentru buget încorporează cifrele respective (fără dezbatere) în recomandările sale legate de buget.
6. Plenul parlamentului se pronunță prin vot asupra bugetului total prezentat de guvern.

Competențele de investigare și de acces la informații

Legea atribuie Comisiei pentru chestiuni confidențiale o puternică autoritate de investigare și un acces extins la informații clasificate, inclusiv competența de a verifica

[21] German Federal Budget Code [Codul bugetului federal german], Articolul 10(a). A se vedea și Hans De With și Erhard Kathmann, „Parliamentary and Specialised Oversight of Security and Intelligence Agencies in Germany" [„Supravegherea parlamentară și specializată a agențiilor de securitate și de informații în Germania"], în *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, Wills și Vermeulen, Anexa A, pp. 225–226.

toate dosarele și documentele aflate sub controlul serviciilor de informații și de a inspecta toate incintele serviciilor. Comisia poate obliga oficiali ai serviciilor și membri ai executivului să răspundă la întrebări și poate apela la experți externi care să îi acorde asistență dacă este necesar.

Date fiind aceste limitări, monitorizarea execuției bugetare, efectuată de parlament, se bazează, de obicei, pe informații puse la dispoziție proactiv (adică, fără a fi solicitate) de executiv și de serviciile de informații. Într-adevăr, legislația aplicabilă în multe țări democratice impune ca executivul și/sau serviciile de informații să furnizeze periodic informații legate de finanțele serviciilor.[22] În Italia, de pildă, primului ministru i se cere să raporteze la fiecare șase luni Comisiei parlamentare pentru securitatea Republicii (COPASIR) cu privire la execuția bugetelor serviciilor de informații.[23]

Totodată, parlamentele trebuie să analizeze solicitările de fonduri suplimentare, care apar de-a lungul unui an fiscal. În cazul serviciilor de informații, asemenea solicitări pot avea legătură cu evenimente neprevăzute, așa cum sunt atacurile teroriste. Ca și în situația altor chestiuni legate de execuția bugetară, examinarea unor astfel de solicitări este repartizată, de regulă, comisiei parlamentare pentru supravegherea serviciilor de informații. În Spania, de exemplu, solicitările de fonduri suplimentare sunt verificate de Comisia pentru fonduri secrete, a cărei opinie este adusă la cunoștința plenului, care se pronunță prin vot.[24]

5.3 VERIFICAREA *EX POST* A FINANȚELOR

Verificarea *ex post* a finanțelor agențiilor publice este în principal responsabilitatea mecanismelor interne de audit ale fiecărei agenții (a se vedea Secțiunea 4) și a instituțiilor SAI naționale (a se vedea Secțiunea 6). Totuși, parlamentele joacă un rol în acest proces, verificând munca auditorilor și efectuând propriile lor investigații. La încheierea unui astfel de proces, unele parlamente adoptă o lege pentru „descărcarea bugetară” (adică, aprobă oficial bilanțurile contabile ale guvernului pentru o perioadă dată).

[22] Pentru o discuție mai detaliată, a se vedea Wills și Vermeulen, pp. 129–131.

[23] Italia, Legea 124/2007, Articolele 33(8) și 29(2).

[24] Spania, Legea 11/1995, Articolul 2.2. A se vedea și Susana Sanchez Ferro, „Parliamentary and Specialised Oversight of Security and Intelligence Agencies in Spain” [„Supravegherea parlamentară și specializată a agențiilor de securitate și de informații în Spania”], în *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, Wills și Vermeulen, Anexa A, p. 271.

5.3.1 Mecanismele parlamentare pentru verificarea *ex post*

Comisiile parlamentare pentru finanțe publice sau pentru audit public (PAC), care efectuează verificarea *ex post* a finanțelor organismelor publice, nu sunt, de obicei, responsabile pentru verificarea *ex post* a finanțelor serviciilor de informații, datorită naturii sensibile a acestora. În schimb, multe parlamente adoptă măsuri speciale pentru verificarea finanțelor serviciilor de informații. De exemplu, în Marea Britanie, rapoartele și avizele Oficiului Național de Audit (instituția supremă de audit din stat) cu privire la serviciile de informații sunt prezentate numai președintelui Comisiei pentru finanțe publice.[25] În schimb,

Caseta 6: Rolul Comisiei britanice pentru informații și securitate în verificarea *ex post*

Comisia pentru informații și securitate a parlamentului Marii Britanii (ISC) include membri din ambele camere. Mandatul ei este de a supraveghea „politicile, administrarea și cheltuielile” serviciilor de informații și de securitate.[26]

Potrivit acestui mandat, ISC efectuează verificarea ex post a finanțelor serviciilor, în principal pe baza avizelor și rapoartelor anuale de audit, pregătite de Oficiul Național de Audit (NAO). Ca parte a procesului, ISC audiază reprezentanții NAO și pe cei ai conducerii superioare a serviciilor pe tema auditului efectuat de NAO.

În propriul său raport anual, ISC include o evaluare a finanțelor serviciilor.[27] Într-o primă etapă, ISC își prezintă raportul primului ministru, însă, ulterior, raportul devine public.[28] În plus, ISC folosește un staff cu atribuții de investigare, care poate primi oricând sarcina de a examina, printre altele, aspecte ale activității serviciilor, care au implicații financiare importante.[29]

---

[25] Președintele Comisiei pentru finanțe publice este întotdeauna un membru al opoziției.

[26] Marea Britanie, Intelligence Services Act [Lege privind serviciile de informații] 1994, Secțiunea 10(1).

[27] A se vedea, de exemplu, Marea Britanie, Comisia pentru informații și securitate, *Annual Report 2010–2011* [*Raport anual 2010–2011*], CM 8114 (2011), pp. 12–16.

[28] Ian Leigh, „Parliamentary and Specialised Oversight of Security and Intelligence Agencies in the United Kingdom” [„Supravegherea parlamentară și specializată a agențiilor de securitate și de informații în Marea Britanie”], în *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, Wills și Vermeulen, Anexa A, p. 298.

[29] Ibid., p. 297; exemple din activitatea de investigare sunt menționate în Marea Britanie, Comisia pentru informații și securitate, *Annual Report 2010–2011* [*Raport anual 2010–2011*], pp. 7, 16, 17 și 79.

principala responsabilitate pentru verificarea lor revine Comisiei pentru informații și securitate, al cărei mandat de supraveghere include verificarea *ex post* a finanțelor serviciilor de informații (a se vedea Caseta 6). În alte țări, de exemplu în Germania (a se vedea Caseta 5), parlamentele au o comisie specială care îndeplinește sarcinile parlamentului în privința bugetelor și bilanțurilor ce conțin informații clasificate.

5.3.2 Procesul și scopul verificării *ex post*

Verificarea parlamentară *ex post* a finanțelor serviciilor de informații se axează în mod normal pe rapoartele instituțiilor SAI. Parlamentarii responsabili pentru verificarea *ex post* analizează și rapoartele anuale și situațiile financiare pregătite de serviciile de informații.[30] O importantă parte a procesului o constituie audierile, în cadrul cărora auditorii SAI, oficiali din executiv și conducerea serviciilor de informații depun mărturie.

Scopul principal al verificării *ex post* este de a determina dacă serviciile de informații: [31]

- au pus în aplicare bugetele în maniera autorizată de parlament la începutul ciclului bugetar.
- au cheltuit fondurile publice și au justificat aceste cheltuieli în conformitate cu legile și politicile aplicabile.
- și-au desfășurat activitatea în mod eficace și eficient.
- au atins obiectivele aferente politicilor, stabilite la începutul ciclului bugetar (dacă se utilizează bugetarea pe bază de performanțe).

La încheierea procesului de verificare, parlamentarii care au efectuat-o pot prezenta un raport conținând recomandări pentru ameliorarea practicilor financiare și a mecanismelor de control ale serviciilor. În unele țări (precum Franța, Germania și Ungaria), unde legea impune ca întregul parlament să aprobe descărcarea bugetară, asemenea rapoarte pot influența votul în plen.

Informațiile obținute cu ocazia verificării *ex post* pot fi utile parlamentarilor la aprobarea bugetelor viitoare. Într-adevăr, parlamentarii își pot utiliza competențele bugetare *ex ante* pentru a obliga executivul și serviciile de informații să accepte recomandările lor *ex post*. Această pârghie funcționează mai bine atunci când există legături puternice între aprobarea *ex ante* a buge-

[30] OCDE, *Relations Between Supreme Audit Institutions and Parliamentary Committees* [*Relațiile dintre instituțiile supreme de audit și comisiile parlamentare*], Sigma Papers, Nr. 33 (Paris: OECD Publishing, ianuarie 2002), pp. 19–20.

[31] În unele țări, verificarea parlamentară *ex post* stabilește și dacă SAI și-au efectuat auditul în mod corespunzător.

telor și verificarea *ex post* a execuției lor. Ceea ce poate fi cel mai bine obținut prin desemnarea unei singure comisii parlamentare care să fie responsabilă pentru ambele funcții în ceea ce privește serviciile de informații (așa cum este cazul Germaniei, a se vedea Caseta 5). Alternativ, coordonarea poate fi intensificată prin întruniri comune ale comisiilor și alte forme de schimb de informații între comisiile responsabile pentru examinarea *ex ante* a bugetului și cele responsabile pentru verificarea *ex post*.

5.3.3 Solicitarea rapoartelor din partea SAI

În unele țări (precum Franța și SUA), parlamentul poate trasa unei instituții SAI sarcina de a investiga un anumit program sau o anumită cheltuială sau de a estima raportul cost-eficacitate aferent unei anumite investiții.[32] Acordarea unei asemenea competențe parlamentului poate contribui la asigurarea faptului că munca SAI sprijină activitatea comisiilor parlamentare de supraveghere. Pe de altă parte, ea poate să ducă la suprasolicitarea SAI și la politizarea activității acesteia (dacă, de exemplu, parlamentari cu influență dau dispoziții SAI să investigheze o problemă din rațiuni partizane). În consecință, în Franța, legea limitează numărul cererilor pe care parlamentul le poate adresa și lasă posibilitatea ca una sau mai multe cereri să fie respinse de Curtea de Conturi. În mod similar, legea germană permite parlamentului să solicite Curții Federale de Audit (FCA) o investigare, dar nu acordă parlamentului puterea de a obliga FCA să facă investigații, păstrând astfel independența acestei instituții.[33]

6. INSTITUȚIILE SUPREME DE AUDIT

În orice țară democratică, există o formă de SAI autonomă, responsabilă cu auditarea agențiilor publice, inclusiv a serviciilor de informații. Deși instituțiile SAI se concentrează în principal asupra aspectelor financiare ale activității guvernamentale, auditul lor se poate extinde și asupra altor aspecte ale unui serviciu guvernamental. O discuție completă cu privire la diferitele tipuri de SAI depășește sfera acestui instrument, dar se poate remarca pe scurt faptul că SAI se împart în două mari categorii: modelul „curții" (precum Curtea de Conturi franceză) și modelul „oficiului" (precum Oficiul Național de Audit din Marea Britanie și Oficiul Guvernamental de Conturi din SUA). Indiferent de forma lor specifică, SAI reprezintă de obicei principalul organism extern responsabil

[32] Franța, Ministerul pentru buget, finanțe publice și funcția publică *Guide to the Constitutional Bylaw on Budget Acts* [*Ghid al legii organice privind legile de finanțe*] (2008) p. 32; (Franța, LOLF), Articolul 54 și Articolul 58; SUA, website-ul Oficiului Guvernamental de Conturi (disponibil la http://www.gao.gov/about/index.html).

[33] Germania, Ministerul Federal de Finanțe, *The Budget System of the Federal Republic of Germany* [*Sistemul bugetar al Republicii Federale Germania*] (Berlin: 2008), p. 47.

pentru verificarea *ex post* a finanțelor serviciilor de informații. Aspectele prezentate în această secțiune se aplică ambelor tipuri de SAI.

6.1 INDEPENDENȚA

Pentru ca SAI să-și ducă la îndeplinire sarcinile cu eficacitate, au nevoie să fie complet independente față de executiv și de toate entitățile pe care le controlează. În fapt, Adunarea Generală a Națiunilor Unite a adoptat o rezoluție ce recunoaște importanța independenței instituțiilor SAI.[34] În mod specific, este necesar ca SAI să aibă:

- *Independență organizațională*
  SAI trebuie înființate prin lege ca instituții autonome, cu buget propriu.
- *Independență operațională*
  SAI trebuie să aibă libertatea de a determina ce controlează, cum și când efectuează auditul, precum și care sunt constatările și recomandările pe care le fac în urma auditului respectiv. Munca auditorilor trebuie protejată împotriva ingerinței oricărui alt organism.
- *Independența personală*
  Independența personală se referă la poziția auditorilor înșiși. Oficialii de rang superior ai SAI trebuie să fie numiți într-un mod care să promoveze selecția unor persoane cu expertiză adecvată și care nu au niciun fel de afilieri sau interese ce ar putea compromite poziția lor ca auditori. Ceea ce impune un proces transparent, incluziv și bazat pe merite, în cadrul căruia candidații trebuie să fie susținuți atât de executiv, cât și de parlament. Odată numiți, auditorilor trebuie să li se garanteze independența în baza legii, prin mandate cu durată fixă și alte măsuri care să îi ferească de represalii în situația în care constatările lor se dovedesc nefavorabile executivului în exercițiu. În fine, auditorii de rang superior trebuie să evite activitățile politice sau de afaceri care le-ar putea compromite independența și/sau ar putea fi percepute ca un conflict de interese.

6.2 FUNCȚII

Principalele funcții ale SAI sunt:

[34] Rezoluția Adunării Generale a Națiunilor Unite, „Promoting the efficiency, accountability, effectiveness and transparency of public administration by strengthening supreme audit institutions” [„Promovarea eficienței, responsabilității, eficacității și transparenței în administrația publică prin întărirea instituțiilor supreme de audit”], United Nations Document A/RES/66/209 (15 martie 2012).

- evidențierea problemelor privind legalitatea, eficiența, eficacitatea în gestiunea financiară, precum și alte abateri de la normele acceptate.
- elaborarea unor recomandări pentru ameliorarea gestiunii financiare, inclusiv controalele interne, gestionarea riscurilor și sistemele de evidență contabilă.
- certificarea, în fața parlamentului, a exactității și corectitudinii cheltuielilor bugetare, contribuind astfel la asigurarea faptului că executivul respectă voința parlamentului.
- asigurarea opiniei publice că banii sunt cheltuiți legal, adecvat, eficient și cu eficacitate.
- tragerea la răspundere a agențiilor guvernamentale pentru modul în care au utilizat banii publici.

În vreme ce multe din aceste funcții sunt exercitate *ex post* – presupunând verificarea activităților financiare după ce acestea au avut loc –, SAI pot avea și un rol *ex ante*. Și anume, o instituție SAI (precum Curtea Federală de Audit din Germania, a se vedea Caseta 7) poate fi mandatată să emită avize cu privire la proiectele de buget.[35] Ceea ce poate fi considerată o funcție preventivă, destinată identificării și remedierii problemelor financiare înainte ca acestea să apară. De pildă, o instituție SAI ar putea recomanda alocarea unor fonduri suplimentare unei anumite activități sau categorii de cheltuieli dacă, în timpul controalelor sale anterioare, au fost identificate constant depășiri de cheltuieli în respectivele cazuri.

În responsabilitatea SAI nu intră depistarea cazurilor de fraudă ori corupție; însă dacă se descoperă dovezi ale unor asemenea practici, SAI trebuie să le prezinte membrilor responsabili din executiv și/sau agențiilor împuternicite cu aplicarea legii.

6.3 AUDITAREA SERVICIILOR DE INFORMAȚII

SAI trebuie să realizeze auditul pentru serviciile de informații folosind aceleași norme pe care le aplică în auditul altor agenții publice, iar jurisdicția SAI trebuie să se extindă asupra tuturor aspectelor legate de finanțele acestor servicii. Nu trebuie să se permită executivului scutirea niciunei zone a activității de informații de supravegherea financiară externă, deoarece o astfel de abordare subminează independența SAI și, totodată, mărește riscul ca întrebuințarea ilegală și incorectă a banilor să fie camuflată.[36]

---

[35] Ibid., p. 18.

[36] Acesta este cazul în SUA, unde autoritatea GAO de a audita mai multe zone din activitatea CIA este restricționată și în practică și prin lege. A se vedea *Intelligence*

Caseta 7: Curtea Federală de Audit a Germaniei

Curtea Federală de Audit a Germaniei (FCA) are sarcina de a audita toate organismele guvernului federal, inclusiv serviciile federale de informații.[37]

Funcții

Funcțiile FCA în raport cu organismele guvernului federal includ:

- auditarea veniturilor, cheltuielilor, activelor și pasivelor lor și examinarea oricăror acțiuni pe care le-au întreprins și care pot avea consecințe financiare.
- sprijinirea parlamentului în exercitarea dreptului său de a stabili bugetele agențiilor, inclusiv prin prezentarea de avize asupra proiectelor de buget.
- sprijinirea parlamentului în adoptarea deciziei privind descărcarea executivului în ceea ce privește gestionarea fondurilor publice.[38]

Sfera auditului

Legea de reglementare nu impune nicio restricție activității FCA. În consecință, FCA este singura care decide ce agenții va audita, când și cum va avea loc controlul. Parlamentul – în acest context, Comisia pentru chestiuni confidențiale din Bundestag – poate solicita efectuarea unui audit de către FCA, dar nu o poate obliga să dea curs solicitării. Auditul FCA stabilește dacă agențiile au respectat legile și reglementările privind activitatea financiară. El stabilește, în special, dacă:

- au fost respectate prevederile legii bugetului.
- evidențele veniturilor, cheltuielilor, activelor și pasivelor agenției sunt corecte și susținute corespunzător de documente.

Community Directive, No. 114 [Directiva nr. 114 privind comunitatea de informații], 30 iunie 2011; Gene Dorado (Controlorul General din SUA), Scrisoare adresată Directorului pentru Informații Naționale James Clapper, referitoare la „GAO Comments on Intelligence Community Directive Number 114: Comptroller General Access to Intelligence Community Information” [„Comentariile GAO cu privire la Directiva nr. 114 privind comunitatea de informaţii: accesul Controlorului General la informațiile deținute de comunitatea de informații”], 28 aprilie 2011; și SUA, GAO, „Central Intelligence Agency: Observations on GAO Access to Information on CIA Programs and Activities” [„Agenția Centrală de Informații: observații privind accesul GAO la informații despre programele și activitățile CIA”], GAO-01-975T (iulie 2001), pp. 4–8.

[37] German Basic Law [Legea fundamentală germană], Articolul 114(2); Germania, Federal Budget Code [Codul bugetului federal] din 19 august 1969, în *Federal Law Gazette I*, p. 1284, ultima dată amendat de Articolul 4 din the Act of 31 July 2009 [Legea din 31 iulie 2009], în *Federal Law Gazette I*, p. 2580, Secțiunea 10a (3); Secțiunea 88.

[38] German Basic Law [Legea fundamentală germană], Articolul 114(2); Regulile de audit ale Bundesrechnungshof (Curtea Federală de Audit a Germaniei), ultima dată amendate prin deciziile Senatului în 29/30 august 2005, Articolele 3, 56–57.

- fondurile publice au fost administrate în mod eficient.
- sarcinile trasate au fost îndeplinite în mod eficace.

Problemele identificate de FCA în domeniul intelligence sunt analizate de Comisia pentru chestiuni confidențiale (a se vedea Caseta 5) ca parte a procesului de descărcare bugetară și a dezbaterilor ulterioare asupra bugetului. Prin urmare, reprezentanții SAI participă frecvent la întrunirile Comisiei pentru chestiuni confidențiale, stabilind o legătură utilă între procesele de audit și cele de alocare de fonduri.[39]

Structura

FCA este condusă de un președinte și un vicepreședinte. Amândoi sunt numiți de executiv și aleși de parlament. Fiecare dintre ei poate avea un mandat de maximum 12 ani. FCA este structurată în departamente pe domenii, fiecare fiind condus de un director și un adjunct. Toate aceste persoane sunt „membri ai Curții," ceea ce înseamnă că se bucură de independență judecătorească. Cele mai multe decizii legate de audit sunt luate în „colegii" formate din câte doi membri ai Curții (directorul cu atribuții în domeniu și șeful de secție); acolo unde nu se ajunge la un acord, președintele li se alătură alcătuind un colegiu din trei membri.[40]

Accesul la informații

Legea obligă toate agențiile guvernamentale, inclusiv serviciile de informații, să furnizeze Curții Federale de Audit orice document pe care aceasta îl consideră necesar pentru a-și desfășura activitatea. Nu există nicio limitare a acestei obligații.[41]

Rapoartele

Cu toate că rapoartele FCA sunt, de regulă, publice, rapoartele privind serviciile de informații nu devin publice. În schimb, sunt prezentate Comisiei pentru chestiuni confidențiale, comisia de supraveghere a serviciilor de informații din Bundestag, precum și organismelor relevante din executiv.[42]

Unele țări (precum Franța ori SUA) scutesc anumite operațiuni contabile ale serviciilor de informații de auditul SAI. În asemenea situații, o bună practică

---

[39] Germania, Federal Budget Code [Codul bugetului federal], Secțiunea 10a (3) și Secțiunile 89–90; Regulile de audit ale Bundesrechnungshof, Articolele 4–5; The Budget System of the Federal Republic of Germany [Sistemul bugetar al Republicii Federale Germania], pp. 49 și 51.

[40] German Federal Court of Audit Act [Lege privind Curtea Federală de Audit germană] din 11 iulie 1985 (BGBl. I 1985, p. 1445, ultima dată amendată de Articolul 17, Act of 9 July 2001 [Legea din 9 iulie 2001] (BGBI. I, p. 1510), Secțiunile 3, 5, 6, 9 și 19.

[41] Germania, Federal Budget Code [Codul bugetului federal], Secțiunile 10a (3) și 95.

[42] Germania, Federal Budget Code [Codul bugetului federal], Secțiunea 10a (3); Regulile de audit ale Bundesrechnungshof, Articolul 50.

impune ca un alt organism independent să fie desemnat să le controleze. În Franța, operațiunile contabile scutite sunt auditate de Comisia pentru Verificarea Fondurilor Speciale – un grup hibrid compus din parlamentari și auditori.[43] În SUA, operațiunile contabile exceptate, „conturi fără voucher” (cheltuieli decontate numai pe baza certificării de către un membru al executivului) nu pot fi examinate de Oficiul Guvernamental de Conturi (GAO), însă pot fi auditate de comisiile de supraveghere a serviciilor de informații din Congres.[44]

Indiferent de modul de efectuare a verificării, întreaga activitate financiară a serviciilor de informații trebuie supusă auditării de către un organism situat în afara comunității de informații și a executivului. În general, SAI sunt cele mai potrivite organisme pentru efectuarea acestui control.

6.4 TIPURI DE AUDIT

Tipurile de audit efectuate de SAI variază de la o țară la alta, însă următoarele trei tipuri sunt cvasi-universale:

- *Auditul financiar*
  Acesta determină exactitatea și corectitudinea situaţiilor financiare prezentate de agențiile publice.
- *Auditul de conformitate*
  Acesta stabilește dacă veniturile și cheltuielile unei agenții sunt conforme cu legile și reglementările aplicabile, inclusiv cu legile anuale ale bugetului.
- *Auditul performanţei și al raportului cost-eficacitate (value for money – VFM)*
  Acesta stabilește dacă agențiile au fost eficace și eficiente în îndeplinirea mandatelor și obiectivelor lor, cu alte cuvinte, dacă banii contribuabililor, investiți în agenții sub forma fondurilor publice, au fost valorificați corespunzător.

---

43 Franța, Loi n°2001–1275 du 28 décembre 2001 de finances pour 2002 [Legea nr. 2001-1275 din 28 decembrie 2001 a finanțelor pentru 2002], Articolul 154; Franța, Adunarea Națională, *Rapport fait au nom de la Commission des Finances, de l’économie générale et du contrôle budgétaire sur le projet de loi de finances pour 2012: Annexe n° 12,* direction de l’action du gouvernement, publications officielles et information administrative [*Raport făcut în numele Comisiei de finanțe, economie generală și control bugetar cu privire la proiectul de lege a finanțelor pentru 2012: Anexa 12*, Direcția de acțiune guvernamentală, publicații oficiale și informare administrativă] (14 octombrie 2009), pp. 25–27.

44 SUA, Auditing Expenditures Approved Without Vouchers [Auditarea cheltuielilor aprobate fără voucher], U.S. Code 31 §3524.

În ceea ce privește serviciile de informații, SAI efectuează în principal auditul financiar și pe cel de conformitate, punând accentul pe controalele interne financiare, pe gestionarea riscurilor și pe sistemele de evidență contabilă.

Deoarece SAI nu pot verifica fiecare tranzacție financiară făcută de o agenție, cele mai multe dintre ele folosesc o abordare bazată pe risc pentru a evalua validitatea constatărilor lor. Și anume, SAI evaluează riscul ca situaţiile financiare ce le sunt prezentate să fie inexacte. Fac acest lucru prin analizarea, *inter alia*, a procedurilor utilizate de agenție în contabilitate și la întocmirea bilanțului, precum și prin analizarea deficiențelor din controalele interne ale agenției și a deficiențelor din propriile proceduri de verificare ale SAI.

Auditarea performanței serviciilor de informații poate fi foarte dificilă din cauza motivelor discutate în Secțiunea 2 a acestui instrument – în special incertitudinea rezultatelor și caracterul insesizabil al avantajelor, specifice muncii de informaţii. De exemplu, SAI pot considera dificilă evaluarea activităților operaționale (așa cum sunt coordonarea agenților și urmărirea), al căror succes ori eșec este dificil de cuantificat. În consecință, SAI se abțin să evalueze rezultatele din aceste zone.

Totuși, auditul performanței poate conduce la constatări pe care auditul financiar și cel de conformitate nu le pot face. A se remarca, de exemplu, cazul unui proiect major de investiții sau cel al unui program de achiziții pe scară largă, care respectă normele financiare și de conformitate, deoarece a fost justificat corespunzător din punct de vedere contabil și se conformează tuturor legilor și reglementărilor aplicabile. Cu toate acestea, valoarea pe care o produce poate fi mică în raport cu banii cheltuiți – o deficiență care poate fi evidențiată doar prin auditul bazat pe performanță.

Atunci când SAI efectuează un audit de performanță al serviciilor de informații, ele vizează, de obicei, anumite probleme sau teme comune mai multor agenții (a se vedea Caseta 8), așa cum sunt sistemele informatice ori procedurile de emitere a certificatului de securitate.

6.5 ACCESUL LA INFORMAȚII

Este necesar ca SAI să aibă acces neîngrădit la informații atât ca o condiție preliminară pentru realizarea unui audit de înaltă calitate, cât și ca mijloc de garantare a independenței operaționale. Dorința, de înțeles, a unui serviciu de informații de a proteja informații confidențiale împotriva unei dezvăluiri neautorizate nu diminuează nevoia SAI de a obține astfel de informații. Prin urmare, constituie o bună practică acordarea prin lege, pentru SAI, a accesului la *toate* documentele, persoanele și locurile pe care auditorii le consideră necesare pentru munca lor. Acesta e, de exemplu, cazul Africii de Sud (a se vedea

Caseta 8: Auditul performanței în Canada

În 2004, Auditorul General (AG) din Canada a efectuat un audit de performanță la Serviciul Canadian pentru Informații de Securitate și la alte agenții din domeniul intelligence. Acest audit a examinat „conducerea de ansamblu a Inițiativei pentru siguranța publică și combaterea terorismului [și] coordonarea muncii de informații între departamente și agenții și capacitatea acestora de a furniza informații adecvate personalului însărcinat cu aplicarea legii."[45] Auditul a avut loc în urma investițiilor masive în scopul combaterii terorismului, făcute de guvernul canadian după evenimentele din 11 septembrie 2001.

În raportul final de audit, AG a ajuns la concluzia, printre altele, că „guvernul nu a avut un sistem de coordonare care să orienteze deciziile privind investițiile, managementul și dezvoltarea și să-i permită să direcționeze acțiuni complementare către agenții separate."[46] În plus, potrivit AG, „guvernul, în ansamblu, nu a reușit să amelioreze capacitatea sistemelor de informații de securitate de a comunica între ele."[47] În plan mai general, AG a constatat că existau „deficiențe în modul în care informațiile sunt gestionate la nivelul guvernului."[48]

Caseta 9), precum și al Germaniei (a se vedea Caseta 7), unde un astfel de acces include informații privind operațiunile de intelligence în desfășurare. Este esențial, dar nu suficient, ca accesul să fie stipulat în legea (legile) ce reglementează SAI. În plus, legislatorii trebuie să se asigure că legile privind serviciile de informații și informațiile clasificate nu intră în contradicție cu prevederile referitoare la accesul SAI. Totodată, legea trebuie să acorde SAI şi competențe care să susţină obţinerea accesului la informații. Astfel de competențe pot include puterea de a trimite citații, puterea de a percheziționa și sechestra și puterea de a obliga la depunerea unei mărturii sub jurământ sau pe bază de declarație (a se vedea Caseta 9).

În unele state, legea restricționează accesul SAI la informații. De pildă, Oficiul Național de Audit (NAO) din Marea Britanie are un acces limitat la datele referitoare la sursele și metodele folosite în munca de informaţii. Această restricție este limitată și clar precizată și nu a fost gândită pentru a obstrucționa munca NAO. Însă în alte țări, restricțiile legate de accesul SAI la informații sunt mult mai extinse. De pildă, în SUA, legea lasă într-o măsură considerabilă la latitudinea comunității de informații să decidă ce informații va furniza Oficiului Gu-

45 Oficiul Auditorului General al Canadei, *March 2004 Report of the Auditor General of Canada* [*Raportul din martie 2004 al Auditorului General al Canadei*] (2004), Secțiunea 3.2.

46 Ibid., Sec. on 3.3.

47 Ibid., Sec. on 3.4.

48 Ibid., Sec. on 3.5.

Caseta 9: Competențele Auditorului General din Africa de Sud [49]

Auditorul General (AG) din Africa de Sud are competențe solide pe care le poate întrebuința ca să obțină acces la informațiile necesare. Caseta de față rezumă aceste competențe. Trebuie remarcat însă că, în practică, includerea unor astfel de puteri în cadrul legal aplicabil AG nu asigură neapărat furnizarea datelor relevante de către serviciile de informații care doresc să le mențină secrete.[50]

Accesul la informații

Atunci când efectuează un audit, legea acordă AG acces deplin și neîngrădit, în orice moment rezonabil, la:

- orice document, orice înregistrare scrisă sau pe suport electronic, sau orice altă informație aflată în posesia entității auditate, care aduce clarificări cu privire la modul de lucru, activitatea financiară, situația financiară sau performanța entității auditate;
- orice bun care aparține entității auditate sau se află sub controlul ei;
- orice reprezentant al entității auditate sau membru al staffului acesteia.

Competențele de audit

Atunci când efectuează un audit, AG poate:

- să solicite unei persoane să dezvăluie sub jurământ sau pe bază de declarație, verbal sau în scris, informații care pot fi relevante pentru audit, inclusiv informații confidențiale, secrete sau clasificate.
- să chestioneze orice persoană cu privire la asemenea informații.

În plus, la efectuarea unui audit, AG poate obține de la un judecător sau magistrat un mandat pentru:

- a intra în orice proprietate, incintă sau vehicul în temeiul suspiciunii rezonabile că informații relevante sunt păstrate sau ascunse acolo.
- a percheziționa orice proprietate, incintă sau vehicul, precum și orice persoană aflată în incintă sau vehicul pentru a căuta informații potențial relevante.
- a-și însuși orice informații potențial relevante în scopul realizării auditului.

[49] Africa de Sud, Public Audit Act, No. 25 of 2004 [Legea auditului public, nr. 25 din 2004], Secțiunile 15–16.

[50] Africa de Sud, Comisia ministerială de verificare a serviciilor de informaţii, *Intelligence in a Constitutional Democracy: Final Report to the Minister for Intelligence Services, the Honourable Mr Ronnie Kasrils, MP* [*Intelligence într-o democrație constituțională: Raport final în atenția ministrului pentru serviciile de informații, Hon. Mr Ronnie Kasrils, MP*] (10 septembrie 2008) pp. 226–227.

În general, dreptul AG de acces la informațiile de care are nevoie anulează obligațiile serviciilor de informații de a păstra confidențialitatea. De exemplu, se poate impune unei persoane căreia îi este interzisă, în mod obișnuit, dezvăluirea unor informații despre un subiect din domeniul intelligence, să prezinte informațiile respective Auditorului General. În asemenea situații, respectarea solicitării AG nu este considerată o încălcare a obligației acelei persoane de a nu dezvălui datele în cauză.

vernamental de Conturi (GAO), în funcție de fiecare caz în parte.[51] În plus, Oficiului nu îi e permis să acceseze informații privind sursele, metodele și acțiunile sub acoperire asociate „conturilor fără voucher."[52] Limitarea accesului la informații obstrucționează munca GAO și a partenerilor săi din alte state; ea poate avea repercusiuni asupra eficacității și caracterului cuprinzător, trăsături specifice unei supravegheri financiare independente.

Chiar atunci când legea acordă instituțiilor SAI acces deplin și competențe solide de aplicare a legii, e posibil ca aceste puteri să nu fie suficiente pentru a asigura accesul la toate informațiile pe care SAI le consideră relevante. Dată fiind natura confidențială a multor chestiuni din domeniul intelligence, SAI se confruntă cu obstacole practice semnificative în accesarea anumitor tipuri de informații. În special, le este dificil să intervieveze informatori plătiți, să obțină informații despre operațiunile sub acoperire și să verifice existența bunurilor folosite de agenții secreți.

Impactul pe care limitările legale și practice în privința accesului la informații îl au asupra auditului depinde, printre altele, de tipul de audit care se efectuează și de disponibilitatea de a coopera a serviciului de informații vizat. În unele situații, limitarea accesului la informații poate prejudicia considerabil capacitatea unei instituții SAI de a-și desfășura activitatea, subminând integritatea procesului de audit și ducând la un nivel mai scăzut decât cel dorit al siguranței auditului. Într-adevăr, este deosebit de problematic dacă auditorii nu știu că

[51] Intelligence Community Directive, No. 114 [Directiva nr.114 privind comunitatea de informații]; și Gene Dorado, Letter to the Director of National Intelligence James Clapper [Scrisoare adresată Directorului pentru Informații Naționale James Clapper], 28 aprilie 2011.

[52] SUA, GAO, „Central Intelligence Agency: Observations on GAO Access to Information on CIA Programs and Activities" [„Agenția Centrală de Informații: observații privind accesul GAO la informații despre programele și activitățile CIA"], pp. 4–8; Intelligence Community Directive, No. 114 [Directiva nr. 114 privind comunitatea de informații]; și Frederick M. Kaiser, „GAO Versus the CIA: Uphill Battles against an Overpowering Force" [„GAO versus CIA: bătălii dificile împotriva unei forțe covârșitoare"], în *International Journal of Intelligence and Counterintelligence* 15, no. 3 (Toamna 2002): pp. 345–353.

informații care le-ar fi putut schimba concluziile nu le-au fost aduse la cunoștință. În absența unor astfel de informații, este posibil chiar ca ei să emită avize fără rezerve, care să inducă, în mod fals, ideea de certitudine și responsabilitate.

Probleme de acest fel apar, cel mai probabil, în țări în care autoritatea și independența SAI nu au fost pe deplin stabilite și/sau SAI se află într-o relație antagonică în raport cu serviciile de informații pe care le auditează. Dacă o instituție SAI ajunge la concluzia că restricțiile în privința accesului său la informații i-au prejudiciat capacitatea de a emite un aviz corect de audit, normele internaționale în materie impun ca SAI să emită un aviz cu rezerve. Prin susținerea acestei datorii profesionale se asigură faptul că orice limitări legale sau practice privind accesul la informații sunt incluse în avizele și rapoartele privind auditul respectiv.

6.6 PROTECȚIA INFORMAȚIILOR

Pentru ca atât serviciile de informații, cât și executivul să fie sigure că informațiile puse la dispoziția auditorilor vor rămâne confidențiale, multe instituții SAI au înființat unități speciale, care dispun de facilități securizate și staff verificat din punct de vedere al securității, pentru a efectua auditul în domeniul intelligence. (Ca regulă generală, personalul SAI care controlează evidenţele serviciilor de informații trebuie să se supună acelorași standarde de securitate care se aplică personalului serviciilor în cauză, care are acces la aceleași evidenţe, inclusiv obligația legală de a proteja caracterul secret al informațiilor clasificate și al altor informații confidențiale.[53]) Gestionarea cu profesionalism a informațiilor confidențiale generează încredere între SAI și serviciile de informații și mărește probabilitatea ca, în viitor, asemenea informații să fie puse la dispoziția auditorilor cu promptitudine.

6.7 RAPOARTELE

Rapoartele sunt principalul mijloc prin care auditorii fac cunoscute constatările și recomandările lor. Printre cei care primesc rapoartele de audit se numără conducerea serviciilor de informații, oficiali din executiv, parlamentari și membri ai publicului, în general. Adeseori, aceste părți implicate și interesate acționează cu precădere pe baza rapoartelor SAI. Cel mai semnificativ este fap-

[53] A se vedea, de exemplu, Australian Auditor General Act [Legea privind Auditorul General australian], 1997, Secțiunea 36; 31 U.S.C. 716; și OCDE, „The audit of secret and politically sensitive subjects, comparative audit practices” [„Auditul subiectelor secrete și politic sensibile, practici comparative de audit”], Sigma Papers, Nr. 6 (Paris: OECD Publishing, 1996), p. 12.

tul că parlamentarii utilizează rapoartele SAI ca bază pentru propria supraveghere asupra finanțelor serviciilor de informații. În fapt, constatările și recomandările SAI pot avea un impact asupra serviciilor de informații și a executivului, în primul rând, prin intermediul deciziilor parlamentare cu privire la viitoarele bugete.

6.7.1 Caracterul secret

Deoarece rapoartele SAI privind serviciile de informații conțin referiri la informații clasificate, de obicei, versiunile needitate nu sunt făcute publice și nu sunt accesibile nici măcar majorității parlamentarilor. Legea și/sau cutumele limitează, de regulă, categoriile de destinatari ai rapoartelor complete (clasificate) la conducerea superioară a serviciilor, oficialii din executiv, membrii comisiilor parlamentare de supraveghere și, în unele cazuri, membrii comisiilor parlamentare de finanțe/buget.

Deși informațiile sensibile privind securitatea națională, conținute în rapoartele SAI, trebuie, în mod cert, să rămână în cadrul „cercului de secretizare," există multe porțiuni din respectivele rapoarte care pot și trebuie să fie făcute publice. În această privință, Auditorul General din Africa de Sud a afirmat că rapoartele sale privind serviciile de informații trebuie să fie făcute publice, deoarece nimic din ceea ce conțin, dacă ar fi dezvăluit, nu ar prejudicia serviciile sau ar compromite securitatea țării.[54]

Interdicția generală de publicare a auditului serviciilor de informații și clasificarea sistematică a conținutului acestuia sunt incompatibile cu principiile democratice fundamentale ale transparenței, guvernării deschise și libertății de informare. În ceea ce privește acest subiect, constituția sud-africană este deosebit de progresistă, impunând ca toate rapoartele Auditorului General să aibă caracter public, inclusiv cele referitoare la serviciile de informații, sub rezerva eliminării informațiilor sensibile.[55] În general, clasificarea trebuie să fie excepția de la regula generală a publicării și trebuie permisă doar atunci când este necesară pentru a proteja interese legitime de securitate națională.

În nicio situație nu trebuie ca membrii serviciilor de informații sau ai executivului să poată utiliza prevederile privind secretizarea pentru a ascunde folosirea ilegală a fondurilor publice. Constituie o bună practică includerea în legislație a unor dispoziții de anulare, care să permită în mod explicit dezvălui-

---

[54] Africa de Sud, Comisia ministerială de verificare a serviciilor de informaţii, *Intelligence in a Constitutional Democracy* [*Intelligence într-o democrație constituțională*] (10 septembrie 2008), p. 229.

[55] Constitution of the Republic of South Africa, No. 108 [Constituția Republicii Africa de Sud, Nr. 108], 1996, Articolul 188(3).

rea informațiilor clasificate atunci când acest lucru este necesar pentru a face cunoscut un delict. Textul următor din „Legea auditului public” din Africa de Sud descrie o astfel de prevedere:

> (1) Auditorul General trebuie să ia măsurile de precauție necesare pentru a împiedica dezvăluirea informațiilor secrete sau clasificate.
>
> (2) Măsurile luate în condițiile de la subsecțiunea (1) nu pot împiedica dezvăluirea niciunei constatări făcute de Auditorul General sau de un auditor autorizat în privința oricărei cheltuieli neautorizate, a unei cheltuieli incorecte sau a unei cheltuieli neproductive și excesive … sau a oricărei alte conduite incorecte sau infracționale, legate de activitatea financiară a unei entități auditate, însă o asemenea dezvăluire nu poate include fapte care, dacă ar fi făcute publice, ar aduce prejudicii interesului național.[56]

6.7.2 Prezentarea de informații opiniei publice

SAI trebuie să aducă la cunoștință publică cel puțin următoarele tipuri de informații legate de auditul/verificările serviciilor de informații:

- *O listă a controalelor pe care SAI le-au efectuat ori le vor efectua*.
  Fiecare referință poate fi sub simpla formă a unui titlu și a unei scurte explicații.[57]
- *Avizul general de audit cu privire la situaţiile financiare ale serviciului în cauză.*
  Fiind în mod normal un document foarte scurt, avizul general dezvăluie puține informații, dar confirmă că a avut loc o interacțiune cu serviciul respectiv.
- *Versiunile publice ale rapoartelor clasificate*
  SAI trebuie să prezinte versiuni publice ale rapoartelor lor, inclusiv cu privire la auditurile periodice și de performanță care vizează serviciile de informații (a se vedea Caseta 8, de exemplu). Acest lucru se poate face prin editarea (înlăturarea) informațiilor sensibile din versiunile clasificate ale rapoartelor, prin elaborarea unor versiuni separate, cu caracter public, ale rapoartelor sau prin includerea tuturor informațiilor clasificate în anexe care nu sunt făcute publice. În timp ce majoritatea organismelor parlamentare și specializate de suprave-

[56] Africa de Sud, Public Audit Act [Legea auditului public], Secțiunea 18.

[57] Oficiul Național Australian de Audit folosește această practică. Un exemplu al unui asemenea plan de auditare poate fi găsit la adresa: http://www.anao.gov.au/~/media/Files/Audit%20Work%20Programs/2011_Audit_Work_Plan.PDF. Un exemplu de audit NAO în curs poate fi găsit la adresa: http://www.anao.gov.au/Publications/Audits-in-Progress .

ghere prezintă versiuni publice ale rapoartelor lor, o astfel de practică nu este încă răspândită printre instituțiile SAI.

6.8 IMPORTANȚA TRANSPARENȚEI ÎN ACTIVITATEA SAI

În virtutea principiilor guvernanței democratice, publicul trebuie să cunoască pe cât mai mult posibil – dar sub rezerva limitărilor de confidențialitate menționate anterior – despre activitatea instituțiilor SAI și rapoartele acestora cu privire la serviciile de informații. Informarea publicului în ceea ce privește auditarea de către SAI a serviciilor de informații contribuie la creșterea încrederii și susținerii în favoarea atât a serviciilor auditate, cât și a SAI. Promovarea unei percepții pozitive asupra serviciilor de informații – care acționează profesionist, folosesc fondurile publice în mod corespunzător și funcționează în limitele legii – este facilitată dacă populația are siguranța că, în mod real, comunitatea de informații este supusă unui control.

Mai mult, transparența contribuie la spulberarea miturilor legate de serviciile de informații – cu referire, în special, la modul în care utilizează fondurile publice. Ceea ce este necesar cu precădere în țările în care nivelul încrederii în serviciile de informații rămâne scăzut, iar serviciile au antecedente de folosire incorectă a fondurilor. Totodată, transparența este utilă în promovarea și documentarea dezbaterii publice privind rolul pe care trebuie să-l aibă serviciile de informații. Fapt ce poate fi important atunci când guvernele se confruntă cu mari deficite bugetare și trebuie să reducă finanţarea serviciilor publice.

7. RECOMANDĂRI

Cu toate că nu există nicio abordare care să fie considerată „cea mai bună” în cazul supravegherii finanțelor serviciilor de informații, următoarele recomandări, extrase din legi, modele instituționale și practici prezentate în acest instrument, constituie bune practici care pot fi adaptate pentru a corespunde unei multitudini de modele legale și instituționale diferite. Cele mai multe recomandări pleacă de la ipoteza că există deja cadrul legal și instituțional pentru bugetare și auditare și că a fost creat cadrul legal pentru gestionarea și utilizarea fondurilor publice.

Recomandări privind bugetarea și raportarea financiară

- Bugetele serviciilor de informații trebuie să fie „cuprinzătoare”, ceea ce înseamnă că trebuie să acopere întreaga activitate financiară a unui serviciu. Legea trebuie să interzică în mod expres serviciilor să se angajeze în activități financiare care nu sunt incluse în bugetele lor.

- Guvernele trebuie să facă publice cât mai multe informații posibil despre bugetele serviciilor de informații, fără a pune în pericol siguranța publică sau securitatea națională. Ele trebuie să facă publice cel puțin suma totală alocată unui serviciu, subtotalurile pentru anumite categorii de costuri, precum și obiectivele asociate anumitor cheltuieli. Informațiile bugetare trebuie clasificate numai atunci când secretizarea este strict necesară pentru a proteja interesele naționale legitime de securitate.
- Parlamentele trebuie să adopte legislația care să reglementeze ce informații financiare (inclusiv bugetele și situaţiile financiare) trebuie făcute publice și care anume pot rămâne confidențiale și/sau supuse unor proceduri extraordinare de raportare și auditare.
- Serviciile de informații trebuie să elaboreze versiuni publice ale situaţiilor lor financiare, care să conțină cât mai multe informații posibil.

Recomandări privind controalele financiare interne

- Serviciile de informații nu trebuie exceptate de la legile care reglementează controalele financiare și mecanismele de auditare interne ale agențiilor publice.
- Dacă, ocazional, unui serviciu de informații i se permit abateri de la legile și reglementările cu privire la gestionarea și utilizarea fondurilor publice, autoritatea care aprobă astfel de abateri trebuie stabilită prin lege.

Recomandări privind supravegherea financiară externă

- Legea trebuie să impună instituțiilor SAI să controleze finanțele serviciilor de informații pentru a stabili dacă situaţiile lor financiare sunt exacte și corecte, dacă tranzacțiile lor financiare respectă legile și reglementările aplicabile și dacă fondurile publice au fost întrebuințate într-o manieră care asigură un raport optim cost-eficacitate. Pentru a realiza aceste obiective, SAI trebuie să aibă competența de a controla toate aspectele activității serviciilor, inclusiv evidențele contabile speciale, referitoare la operațiuni sub acoperire sau sensibile din alte puncte de vedere.
- Parlamentele și SAI trebuie să supună finanțele serviciilor de informații aceluiași nivel de verificare pe care îl aplică în cazul altor agenții publice. Această verificare trebuie să aibă loc pe parcursul ciclului bugetar, începând cu analiza completă a secțiunilor clasificate din propunerile de buget și încheind cu verificarea *ex post* și auditarea evidențelor financiare ale serviciilor.
- Legea trebuie să acorde organismelor externe de supraveghere acces la toate informațiile pe care acestea le consideră necesare pentru a-și

desfășura activitatea și care sunt deținute fie de serviciul de informații auditat, fie de un alt organism public. Un astfel de acces trebuie susținut prin competențe de investigare adecvate, suficient de puternice pentru a obliga la dezvăluirea informațiilor respective.

- Parlamentele și SAI care dispun de acces la informații confidențiale trebuie să ia măsuri pentru protejarea acestor informații împotriva unei dezvăluiri neautorizate. Astfel de măsuri trebuie să asigure faptul că informațiile în cauză sunt disponibile numai pentru personalul care trebuie să le cunoască, sunt securizate fizic și tehnologic și că sunt instituite sancțiuni pentru a descuraja dezvăluirea neautorizată.
- Membrii comisiilor parlamentare cu responsabilități de supraveghere financiară trebuie să aibă suficiente resurse, atât umane, cât și tehnologice, care să le permită să înțeleagă finanțele serviciilor de informații și să efectueze verificări de substanță.
- Parlamentele trebuie să se asigure că SAI au autoritatea și resursele necesare pentru a-și desfășura activitatea. Mai mult, ele trebuie să promoveze punerea în aplicare a recomandărilor SAI de către serviciile de informații.
- Parlamentele trebuie să se asigure că există legături corespunzătoare între organismele externe de supraveghere în așa fel, încât rezultatele verificărilor *ex post* și ale auditului să poată fi folosite ca informații de suport în examinarea proiectelor de buget din anii următori.
- Comisiile parlamentare responsabile cu supravegherea financiară a serviciilor de informații trebuie să colaboreze activ cu SAI. Această colaborare ar trebui să includă examinarea rapoartelor lor, organizarea unor întâlniri de evaluare și adoptarea măsurilor necesare prin care să se asigure că SAI dispun de competențele și resursele adecvate pentru auditarea serviciilor de informații.
- Parlamentele și SAI au responsabilitatea de a informa constant populația cu privire la supravegherea pe care o efectuează în cazul serviciilor de informații. Ele trebuie să elaboreze versiuni publice ale constatărilor lor și să prezinte periodic opiniei publice rapoarte despre activitățile pe care le desfășoară.

INSTRUMENTUL 9

Gestionarea reclamațiilor privind serviciile de informații

Craig Forcese



9

Gestionarea reclamațiilor privind serviciile de informații

Craig Forcese

1. INTRODUCERE

Acest instrument se axează pe rolul jucat de organismele de supraveghere în gestionarea reclamațiilor din partea publicului la adresa serviciilor de informații, precum și a reclamațiilor din partea membrilor serviciilor de informații. Un sistem de gestionare a reclamațiilor este în mod special necesar în cazul serviciilor de informații, fiindcă acestora „li se încredințează deseori puteri excepționale, precum urmărirea sau eliberarea certificatului de securitate, care, dacă sunt folosite incorect sau greșit, atrag riscul nedreptățirii grave a unor persoane.”[1] Cu toate acestea, justificarea unui sistem de gestionare a reclamațiilor depășește cu mult sfera remediilor pentru încălcarea unor drepturi. În cazul serviciilor de informații, mecanismele de gestionare a reclamațiilor „pot contribui și la creșterea responsabilității prin evidențierea unor deficiențe administrative și a unor lecții de reținut, determinând, astfel, îmbunătățirea rezultatelor.”[2]

Din aceste motive și din altele, sistemele de gestionare a reclamațiilor sunt considerate o parte esențială a guvernanței în domeniul intelligence. În acest sens, compilația raportorului special al Națiunilor Unite, de „bune practici” pri-

[1] Hans Born și Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practices for Oversight of Intelligence Agencies* [*Responsabilizarea în domeniul intelligence: standarde legale și cele mai bune practici pentru supravegherea agențiilor de informații*] (Geneva: DCAF, Universitatea din Durham și Parlamentul Norvegiei, 2005), p. 105.

[2] Hans Born și Ian Leigh, *Democratic Accountability of Intelligence Services* [Responsabilitatea democratică a serviciilor de informații], Articol de politică nr. 19 (Geneva: DCAF, 2006), p. 17.

vind serviciile de informații și supravegherea acestora,[3] solicită imperios existența unor proceduri care „să aducă o reclamație în fața unei instanțe sau a unei instituții de supraveghere, așa cum sunt un ombudsman, un comisar pentru drepturile omului sau o instituție națională pentru drepturile omului," ori de câte ori o persoană consideră că drepturile sale au fost încălcate. Mai mult, victimele unor acțiuni ilegale trebuie „să poată face apel la o instituție în măsură să asigure un remediu efectiv, inclusiv deplina reparație pentru prejudiciul suferit."[4] Acest drept la măsuri reparatorii în cazul încălcării drepturilor omului se întemeiază pe legislația internațională privind drepturile omului, care impune, totodată, ca persoanele să aibă dreptul la un „remediu efectiv."[5] Este important de precizat că, în acest context, „remediul efectiv" trebuie interpretat mai mult decât ca o simplă recompensă pentru o încălcare demonstrată a drepturilor. El include și dreptul de a se adresa unei instituții capabile să stabilească pe cale judiciară dacă un drept a fost într-adevăr încălcat.[6]

În continuare, documentul raportorului special solicită imperios ca instituțiile împuternicite să examineze reclamațiile și cererile de obținere a unui remediu să fie independente în raport cu serviciile de informații și cu executivul, ca structură politică, și „să aibă acces deplin și neîngrădit la toate informațiile relevante, la resursele și expertiza necesare pentru efectuarea investigațiilor, precum și competența de a emite dispoziții cu caracter obligatoriu."[7]

Aceste ultime elemente de concepție ridică cele mai dificile probleme. În prezent, există un volum considerabil de date comparative referitoare la modul în

---

[3] Consiliul Națiunilor Unite pentru Drepturile Omului, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight* [*Raportul Raportorului Special pentru promovarea și protejarea drepturilor omului și libertăților fundamentale în contextul combaterii terorismului: Compilație de bune practici privind cadrul și măsurile legale și instituționale, care asigură respectarea drepturilor omului de către agențiile de informații în contextul luptei împotriva terorismului, inclusiv supravegherea acestora*] (de aici înainte numit „Raportul Scheinin")], United Nations Document A/HRC/14/46 (17 mai 2010), p. 10.

[4] Raportul Scheinin, p. 10.

[5] Raportul Scheinin, p. 11 – citând Articolul 2 din the *International Covenant on Civil and Political Rights* [*Convenția internațională cu privire la drepturile civile și politice*].

[6] *Klass v. FRG* [Klass versus Republica Federală Germania], A 28 (1979), 2 EHHR 214 la paragraful 64 – interpretând Articolul 13 din *European Convention on Human Rights* [*Convenția europeană a drepturilor omului*].

[7] Raportul Scheinin, p. 11.

care sunt concepute organismele de gestionare a reclamațiilor și sfera lor de acțiune în sectorul intelligence. Deși este imposibil, cu resursele disponibile pentru acest proiect, să se evalueze activitatea efectivă a acestor entități, se pot trage unele concluzii pornind de la structura, sfera de acțiune și competențele lor. Această trecere în revistă evidențiază faptul că, deși nevoia de sisteme de gestionare a reclamațiilor este acută, conceperea unui sistem eficace poate ține mai mult de artă decât de știință. Statele trebuie să se decidă dacă se vor baza pe instanțe convenționale sau vor concepe organisme speciale pentru gestionarea reclamațiilor. Dacă optează pentru cea de-a doua variantă, statele ar putea fi în măsură să conceapă un regim special de gestionare a informațiilor, care să se ocupe de problemele cu totul speciale de secretizare și securitate, specifice reclamațiilor ce vizează domeniul intelligence. În același timp, atunci când se recurge la organisme specializate de gestionare a reclamațiilor, apar alte probleme legate de modul în care ele trebuie concepute și, nu în cele din urmă, probleme legate de jurisdicție, componență și competențe de acordare a remediilor.

Instrumentul de față examinează aceste subiecte, structurând prezentarea în mai multe secțiuni diferite: înaintarea reclamațiilor; locurile în care se depun reclamațiile; procedura de gestionare a reclamațiilor și de verificare a informațiilor; și remediile acordate în urma reclamațiilor.

2. ÎNAINTAREA RECLAMAȚIILOR

Regulamentele stabilesc cine are competența de a înainta reclamații. În ceea ce privește serviciile de informații, reclamațiile pot fi împărțite în două categorii: prima – reclamațiile „din interior"; și a doua – reclamațiile „publice." În accepțiunea capitolului de față, reclamațiile „din interior" sunt cele înaintate unui organism independent de angajați din domeniul intelligence sau de alți angajați guvernamentali, afectați de o acțiune a serviciului de informații. Reclamațiile „publice" sunt înaintate de persoane, care nu au legături cu comunitatea de informații sau cu guvernul.

2.1 RECLAMAȚIILE DIN INTERIOR

În unele jurisdicții, angajații serviciilor de informații sau alți angajați guvernamentali pot înainta plângeri împotriva unui serviciu de informații. Asemenea reclamații din interior au legătură uneori cu modul în care reclamantul e tratat de serviciu. De pildă, în Canada, Serviciul Canadian pentru Informații de Securitate (CSIS) efectuează aproape toate verificările de securitate la nivelul guvernului în vederea acordării certificatelor de securitate pentru angajații guvernamentali. Un angajat nemulțumit de rezultatul procesului de verificare poate depune o reclamație la un organism administrativ independent (sau organism

specializat de supraveghere), denumit Comisia de Verificare a Informațiilor de Securitate (SIRC).[8]

În alte cazuri, reclamațiile „din interior” pot fi mai generale şi reprezintă raportări ale unor fapte reprobabile sau excese ale serviciilor de informații. De exemplu, în Belgia, serviciul de investigare al Comisiei Permanente pentru Verificarea Agențiilor de Informații (cunoscută, de obicei, drept Comisia I) e autorizat:

> … să analizeze reclamațiile și denunțurile unor persoane care au fost direct afectate de intervenția unui serviciu de informații … Orice funcționar public, orice persoană care îndeplinește o funcție publică și orice membru al forțelor armate, direct afectați de dispoziții, decizii sau reguli aplicabile lor, precum și de metode sau acțiuni, pot depune o reclamație …. fără a avea nevoie să ceară o autorizație din partea superiorilor lor.[9]

În conformitate cu legislația SUA, un angajat sau un contractor al CIA trebuie să parcurgă un proces intern de notificare înainte de a depune o reclamație la comisiile de supraveghere din Congres. Legea de reglementare stipulează, totodată, că un asemenea reclamant din interior, „care intenționează să aducă la cunoștința Congresului o reclamație sau informații referitoare la o preocupare urgentă, poate înainta astfel de reclamație sau informații Inspectorului General.”[10] „Preocupare urgentă,” în acest context, înseamnă:

- O problemă gravă sau flagrantă, un abuz, o încălcare a legii ori a unui ordin sau o deficiență legată de finanțarea, administrarea sau operațiunile aferente unei activități de intelligence care implică date clasificate, dar nu se referă la diferențe de opinie în chestiuni de politici publice.
- O declarație falsă în fața Congresului ori fapta de a nu aduce la cunoștința acestuia, în mod deliberat, o chestiune sau un fapt concret

[8] Canadian Security Intelligence Service Act [Lege privind Serviciul Canadian pentru Informații de Securitate] (31 august 2004), R.S.C., Capitolul C-23, Secțiunea 42 (disponibil la http://www.csis-scrs.gc.ca/pblctns/ct/cssct-eng.asp).

[9] Belgia, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment [Lege pentru reglementarea verificării poliției și serviciilor de informații și a Unității de Coordonare pentru Evaluarea Amenințărilor] (18 iulie 1991), Articolele 28 și 30 (disponibil la www.comiteri.be/images/pdf/engels/w.toezicht-l.contrle-engelseversie.pdf).

[10] SUA, Inspector General for the Central Intelligence Agency [Inspectorul General pentru Agenția Centrală de Informații], U.S. Code 50, §403q (e) (2) (disponibil la http://codes.lp.findlaw.com/uscode/50/15/I/403q).

legat de finanțarea, administrarea sau modul de operare într-o activitate de intelligence.[11]

Reclamațiile din interior de acest gen sunt o formă de „denunț intern" – prin intermediul lor sunt aduse la cunoștință fapte reprobabile, fără a se parcurge ordinea ierarhică din serviciile de informații, însă fără a împărtăși, neapărat, secrete în afara cadrului restrâns al agențiilor guvernamentale sau al altor organisme de supraveghere aprobate. Existența unor astfel de mecanisme de reclamare poate reduce probabilitatea ca un angajat să recurgă la forme mai radicale de dezvăluire, de exemplu, în mass-media.

Întru totul rezonabil, unele jurisdicții încurajează folosirea acestei forme de denunț intern. De pildă, unele asigură protecția reclamantului din interior care își înaintează reclamația prin intermediul unor astfel de canale autorizate. De exemplu, în Noua Zeelandă, „niciun angajat al unei agenții de informații și securitate, care aduce la cunoștința Inspectorului General (pentru informații și securitate) orice chestiune, nu va fi pedepsit de agenția de informații și securitate și nici nu va fi supus niciunui fel de tratament discriminatoriu, legat de locul său de muncă, numai ca urmare a faptului că a adus acea chestiune la cunoștința Inspectorului General," cu excepția cazului în care a acționat cu rea-credință.[12] În SUA, „în cazul unei astfel de reclamații, nu poate fi întreprinsă nicio acțiune de represalii sau care constituie o amenințare cu represalii de către un angajat al Agenției (Centrale de Informații) aflat într-o poziție care îi permite o asemenea acțiune, cu excepția situației în care reclamația a fost făcută sau informațiile au fost dezvăluite știindu-se că era vorba de un fals ori ignorându-se voit adevărul sau falsitatea celor reclamate."[13]

În unele jurisdicții, denunțul intern este o cerință preliminară pentru formele mai publice, externe, de denunț. De exemplu, în Canada, dacă un reclamant nu face mai întâi o dezvăluire pe canale interne, îi va fi dificil să se apere cu succes

---

[11] SUA, Inspector General for the Central Intelligence Agency [„Inspectorul General pentru Agenția Centrală de Informații"], U.S. Code 50, §403q (d)(5)(G).

[12] Noua Zeelandă, Inspector-General of Intelligence and Security Act [Lege privind Inspectorul General pentru Informații și Securitate] (1 iulie 1996), Secțiunea 18 (disponibil la http://www.legislation.govt.nz/act/public/1996/0047/latest/whole.html-dlm392526).

[13] SUA, Inspector General for the Central Intelligence Agency [Inspectorul General pentru Agenția Centrală de Informații], U.S. Code 50, §403q (e)(3)(B).

împotriva unor acuzații penale de dezvăluire neautorizată a unor informații clasificate.[14]

2.2 RECLAMAȚIILE PUBLICE

Reclamațiile publice sunt proceduri inițiate de persoane care nu au legături cu guvernul. Aceste tipuri de reclamații sunt mult diferite față de reclamațiile din interior. Unul dintre motive ar fi că persoana care face o reclamație publică poate avea doar informații vagi despre delictul respectiv. De pildă, o persoană urmărită pe nedrept poate afla despre această problemă doar din întâmplare și chiar atunci e posibil să nu cunoască identitatea precisă a agenției care îl urmărește. Din acest motiv, persoana respectivă va avea, probabil, puține informații concrete pe care să-și bazeze reclamația. Totodată, este posibil ca acea persoană să provină dintr-un grup social, etnic sau religios care, de regulă, nu recurge la reclamații sau este descurajat ori împiedicat, într-un mod sau altul, să o facă. Un exemplu clasic pentru acest tip de persoană ar putea fi un imigrant recent, nefamiliarizat cu instituțiile și practicile din noua societate gazdă.

În consecință, orice sistem care vizează reclamațiile publice trebuie să admită incertitudinea și să fie larg accesibil. Ceea ce înseamnă că trebuie să se accepte motive foarte generale pentru reclamațiile publice și bariere foarte scăzute pentru demararea investigațiilor ca reacție la reclamațiile respective.

Unele jurisdicții adoptă această practică asigurându-se că nu există restricții cu privire la categoria de persoane îndreptățite să facă reclamații și permițând reclamanților să-și manifeste preocuparea față de o gamă largă de subiecte. De exemplu, în Olanda, după notificarea ministrului cu atribuții în domeniu, care să-i permită acestuia să-și exprime opiniile, „fiecare persoană” poate înainta reclamații instituției ombudsmanului național cu privire la aplicarea, de către serviciile de securitate, a legii care le reglementează activitatea.[15] În Irlanda, Comisia de Ombudsman pentru Garda Siochána poate „primi reclamații făcute de membri ai publicului cu privire la conduita membrilor Garda Siochána” (adică, poliția).[16] În mod asemănător, în Canada, cea mai generală

---

[14] Canada, Security of Information Act [Lege privind siguranța informațiilor] (1985), R.S.C., Capitolul O-5, Secțiunea 15 (disponibil la http://laws.justice.gc.ca/eng/acts/O-5).

[15] Olanda, Intelligence and Security Services Act [Lege privind serviciile de informații și de securitate] (7 februarie 2002), Articolul 83 (amendat) (disponibil la www.ctivd.nl/?download=WIV2002Engels.pdf).

[16] Irlanda, Garda Síochána Act [Lege privind Garda Síochána], 2005, nr. 20 din 2005, Secțiunea 67.

reclamație pe care o poate înainta o persoană împotriva serviciului de informații se referă la „orice act sau lucru făcut de Serviciu.”[17] În fine, în SUA, Inspectorul General al CIA „este autorizat să primească și să investigheze reclamații sau informații din partea oricărei persoane cu privire la existența unei activități ce constituie o încălcare a legilor, regulilor sau regulamentelor ori o administrare incorectă, o risipă substanțială de fonduri, un abuz de autoritate sau un pericol serios și concret la adresa sănătății și siguranței publice.”[18]

Asemenea formulări generale ale motivațiilor pentru reclamațiile publice par de dorit dacă scopul modelului de gestionare a reclamațiilor este acela de a adăuga alte mijloace de reglementare a legalității și probității conduitei serviciilor de informații. Totuși, o serie de jurisdicții se îndepărtează de la acest concept general și restrâng sfera celor în măsură să înainteze reclamații la o categorie de indivizi mai limitată decât aceea pe care o implică formularea „orice persoană.” Unele dintre aceste limitări par modeste, dar pot avea o sferă de cuprindere destul de incertă. De pildă, Comisia pentru Reclamații din Kenya poate primi reclamații de la „orice persoană lezată” de serviciul de informații în exercitarea competențelor sale sau în îndeplinirea funcțiilor sale.[19] În Africa de Sud, „orice membru al publicului” poate înainta o reclamație Comisiei mixte permanente pentru informații „cu privire la ceva considerat de individul respectiv că i-a afectat persoana sau proprietatea și care a fost provocat de un serviciu.”[20]

Ambele abordări par să preîntâmpine reclamațiile anticipative ori speculative, motivate de conștientizarea unei anumite practici a serviciilor de informații. De exemplu, o asociație etnică ce suspectează crearea unui profil etnic în investigațiile serviciilor de informații, ar putea să nu fie în măsură să înainteze o reclamație în absența unui reclamant reprezentativ, care să aibă o experiență personală legată de asemenea practici. Este dificil de apreciat care

---

[17] Canadian Security Intelligence Service Act [Lege privind Serviciul Canadian pentru Informații de Securitate] (31 august 2004), R.S.C., Capitolul C-23, Secțiunea 41 (disponibil la http://www.csis-scrs.gc.ca/pblctns/ct/cssct-eng.asp).

[18] SUA, Inspector General for the Central Intelligence Agency [Inspectorul General pentru Agenția Centrală de Informații], U.S. Code 50, §403q (e)(3).

[19] Kenya, National Security Intelligence Service Act [Legea Serviciului Național pentru Informații de Securitate] (31 decembrie 1998), Secțiunea 24 (disponibil la http://www.nsis.go.ke/act.pdf).

[20] Africa de Sud, Intelligence Services Oversight Act [Lege privind supravegherea serviciilor de informații] (23 noiembrie 1994), Secțiunea 3 (1) (f) (disponibil la http://www.acts.co.za/intelligence_services_oversight_act_1994.htm).

este valoarea adăugată a unei asemenea restricții dacă scopul sistemului de reclamații este de a consolida legalitatea și probitatea serviciului de informații.

Situația e și mai problematică atunci când jurisdicțiile impun reguli legate de naționalitate pentru anumite tipuri de reclamații. De exemplu, Inspectorul General pentru Informații și Securitate din Noua Zeelandă poate primi reclamații numai de la „o persoană neo-zeelandeză" (cetățean sau rezident permanent) sau de la o persoană care a fost sau este angajată de una dintre agențiile de informații.[21] Inspectorul General australian pentru Informații și Securitate (IGIS) poate primi reclamații referitoare la serviciul de informații externe australian numai din partea unei „persoane care e cetățean australian sau rezident permanent."[22] (Asemenea limitări pe criterii de naționalitate nu se aplică, totuși, reclamațiilor care vizează serviciul australian de informații de securitate interne.)

Regulile privind naționalitatea (sau naționalitatea/rezidența) sunt o barieră arbitrară în calea reclamațiilor. Consecința poate fi evitarea unui flux de informații despre activitatea serviciului de informații din partea anumitor grupuri, cel mai probabil grupuri țintă, incluzând reclamații din partea refugiaților și a altor persoane străine, care nu sunt încă rezidenți permanenți sau cetățeni. Și aici, în măsura în care reclamațiile servesc drept semnale de alertă timpurie în privința unor delicte, este dificil să se aprecieze beneficiul pe care îl aduc asemenea limitări.

3. LOCURI ÎN CARE POT FI ÎNAINTATE RECLAMAȚIILE

Această secțiune se referă la locul unde pot fi depuse reclamațiile. Există o varietate de instituții cărora le pot fi înaintate reclamații. În termeni generali, aceste instituții pot fi subdivizate în două mari categorii: locuri generale și locuri specializate. Prin „locuri generale," instrumentul de față înțelege instituții fără un mandat specializat de supraveghere în domeniul securității sau de intelligence. Ca exemple de locuri generale, pot fi menționate instanțele judecătorești, instituțiile de tip ombudsman, comisiile naționale pentru drepturile omului și alte organisme de reglementare, așa cum sunt comisarii pentru protecția datelor. Pe de altă parte, „locuri specializate" sunt instituțiile mandatate anume să se ocupe de probleme din domeniul securității sau de

[21] Noua Zeelandă, Inspector-General of Intelligence and Security Act [Lege privind Inspectorul General pentru Informații și Securitate] (1 iulie 1996), Secțiunea 11.

[22] Australia, Inspector-General of Intelligence and Security Act [Lege privind Inspectorul General pentru Informații și Securitate] (17 octombrie 1986), Secțiunea 8 (disponibil la http://www.comlaw.gov.au/Details/C2011C00349).

intelligence. Exemplele includ organismele specializate de supraveghere precum Comisia I din Belgia și SIRC din Canada.

3.1 LOCURILE GENERALE

3.1.1 Instanțele judecătorești ordinare

În unele jurisdicții, instanțele judecătorești ordinare, cu atribuții în materie civilă, au competența de a examina o reclamație legată de serviciile de informații, motivată prin forme recognoscibile de injustiție civilă (inclusiv diferite forme de delicte civile). În altele, instanțele administrative pot examina cazuri care se circumscriu propriei lor jurisdicții (anume dreptul administrativ) și care se referă la acțiuni ale serviciilor de informații.[23]

În realitate, cel puțin în unele jurisdicții (și probabil în cele mai multe), instanțele judecătorești de un tip sau altul constituie singurul loc în care, conform legii, se pot primi reclamații privind serviciile de informații.[24] În acele jurisdicții, nu există organisme specializate de supraveghere a serviciilor de informații, autorizate să primească reclamații. O astfel de abordare pune anumite probleme. După cum se menționează mai jos, instanțele pot avea competența de a acorda remedii importante, însă, din motive practice, poate fi aproape imposibil pentru un reclamant să obțină un asemenea remediu: reclamațiile, uneori singulare, cu privire la serviciile de informații, sunt înghesuite în jurisdicția convențională a instanțelor judecătorești ordinare (spre exemplu, ca delict civil) sau nu sunt examinate deloc.

---

[23] Consiliul Națiunilor Unite pentru Drepturile Omului, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum* [*Raportul Raportorului Special pentru promovarea și protejarea drepturilor omului și libertăților fundamentale în contextul combaterii terorismului: Addendum*], United Nations Document A/HRC/14/46/Add.1 (26 mai 2010), p. 50 (discuție despre Finlanda).

[24] Consiliul Națiunilor Unite pentru Drepturile Omului, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum*, Paragraful 121 (care numește mecanismul reclamațiilor din Benin ca fiind Curtea constituțională); Paragraful 294 (care numește locul principal de adresare a reclamațiilor în Ecuador ca fiind Curtea Constituțională); Paragraful 243 (idem, în legătură cu Costa Rica); Paragraful 307 (care numește instanțele judecătorești ca fiind principalul mecanism pentru reclamații înaintate de o persoană lezată de urmărirea de către serviciul de securitate); Paragraful 353 (rolul instanțelor judecătorești în raport cu delictele civile comise de serviciile de informații din Georgia și rolul procurorului șef în raport cu delictul penal); Paragraful 482 (despre sistemul din Letonia); Paragrafele 556–557 (despre sistemul din Madagascar).

3.1.2 Organismele convenționale de reglementare

Este important, de asemenea, faptul că serviciile de informații, la fel cu celelalte instituții guvernamentale, intră sub jurisdicția instituțiilor care au fie mandate generale de gestionare a reclamațiilor împotriva organismelor publice, fie mandate tematice, care nu sunt specifice serviciilor de informații. Astfel de entități includ instituțiile de tip ombudsman, comisiile de protecție a datelor și comisiile pentru drepturile omului. Acestea pot fi, de exemplu, împuternicite să examineze reclamații legate de utilizarea informațiilor de către serviciile de informații, sau, mai general, legate de respectarea de către servicii a drepturilor omului. De pildă, în Olanda, ombudsmanului național îi pot fi înaintate reclamații privind, printre altele, acțiuni ale miniștrilor cu responsabilităţi în domeniu, ale șefilor Serviciului General de Informații și Securitate și, respectiv, ale Serviciului pentru Informații de Apărare și Securitate, precum și ale persoanelor care lucrează pentru aceste entități.[25] În mod asemănător, în Finlanda și Suedia, reclamațiile referitoare la poliția de securitate pot fi prezentate instituției ombudsmanului parlamentar.[26] În Belgia, Finlanda și Canada, comisarul pentru viața privată (sau pentru protecția datelor) poate primi reclamații privind modul de gestionare de către serviciile de informații a datelor cu caracter personal.[27]

În unele jurisdicții, legea impune organismelor specifice de reglementare care au competențe pe anumite teme să se consulte cu organismele specializate de supraveghere a serviciilor de informaţii și cu organismele de gestionare a reclamațiilor – prezentate în următoarea secțiune – în cazul în care o reclamație se referă la serviciile de informații și/sau la chestiuni de securitate

[25] Olanda, Intelligence and Security Services Act [Lege privind serviciile de informații și de securitate], Articolul 83.

[26] Consiliul Națiunilor Unite pentru Drepturile Omului, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, p. 49 (despre Finlanda); Comisia de anchetă privind acțiunile oficialilor canadieni în cazul Maher Arar, în *International Models of Review of National Security Activities* (mai 2005), p. 14 (disponibil la http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/eng/IntlModels_may26.pdf).

[27] Consiliul Națiunilor Unite pentru Drepturile Omului, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum*, Paragrafele 67, 75 și 82 (despre Belgia); Paragraful 327 (despre Finlanda); Paragraful 374 (care prezintă rolurile instituției de tip ombudsman din Grecia); a se vedea și Canada, Privacy Act [Lege privind viața privată] (1985), R.S.C., Capitolul P-21, Secțiunea 29 (disponibil la http://laws-lois.justice.gc.ca/eng/acts/P-21/index.html).

națională. De exemplu, în Canada, Comisia Canadiană pentru Drepturile Omului trebuie să repartizeze la SIRC reclamațiile referitoare la practici „bazate pe considerente ce au legătură cu securitatea Canadei." După care, SIRC le investighează și informează Comisia, care decide dacă dă curs reclamației.[28] Acest tip de bifurcare duce inevitabil la complicarea cazurilor, însă este util prin aceea că restrânge numărul entităților implicate în gestionarea informațiilor clasificate. În același timp, se reduce probabilitatea ca gestionarea reclamațiilor să fie subminată prin refuzul serviciilor de informații de a furniza informații clasificate organismelor convenționale de reglementare.

3.1.3 Dezavantaje ale locurilor generale

O preocupare comună în cazul locurilor generale, fie ele instanțe judecătorești sau organisme convenționale de reglementare, este accesul la informațiile clasificate. În unele jurisdicții, instanțele civile pot fi împuternicite să acorde despăgubiri reclamanților care au câștigat în cazurile în care serviciile de informații au comis delicte civile, însă, în practică, solicitările guvernului de păstrare a caracterului secret creează dificultăți în litigiile civile din instanțele ordinare. Deoarece reclamantului îi revine sarcina de a proba delictul civil, controlul exercitat de guvern asupra faptelor relevante poate face aproape imposibilă câștigarea unui litigiu civil.[29] În mod similar, organismele convenționale de reglementare care nu au o misiune specifică în chestiuni ce țin de domeniul intelligence și de securitate națională pot fi în imposibilitatea de a accesa și verifica informații clasificate atunci când investighează reclamații referitoare la serviciile de informații. De exemplu, organismul general pentru gestionarea reclamațiilor publice împotriva forței naționale de poliție a Canadei, Poliția Regală Călare Canadiană, s-a plâns în mod repetat de

[28] Canadian Human Rights Act [Legea canadiană privind drepturile omului] (1985), R.S.C., Capitolul H-6, Secțiunile 45–46 (disponibil la http://laws-lois.justice.gc.ca/eng/acts/H-6/page-15.html).

[29] Pentru cazurile în instanță în care invocarea de către guvern a caracterului secret a prejudiciat (sau, cel puțin, a complicat) capacitatea reclamantului de a obține reparații civile, a se vedea *Mohamed v. Secretary of State for Foreign and Commonwealth Affairs* [*Mohamed versus Secretarul de Stat pentru afaceri externe și Commonwealth*] [2009] EWHC 152 (Admin) (Marea Britanie); *Mohamed v. Secretary of State for Foreign and Commonwealth Affairs* [*Mohamed versus secretarul de Stat pentru afaceri externe și Commonwealth*] [2009] EWHC 2549 (Admin) (Marea Britanie); *Canada (Attorney General) v. Almalki* [*Canada (Procurorul General) versus Almalki*], 2011, FCA 199 (Canada); *Mohamed v. Jeppesen Dataplan, Inc.* [*Mohamed versus Jeppesen Dataplan, Inc.*], 614 F.3d 1070 (9th Cir.Cal. 2010) (SUA).

incapacitatea sa de a examina activitățile poliției privind securitatea națională, din cauza secretizării.[30]

Totodată, este posibil ca locurile generale să fie *prea* generale; cu alte cuvinte, să le lipsească expertiza în materie de servicii de securitate și de informații. Drept consecință, ele pot manifesta mai multă deferență față de motivațiile legate de caracterul secret sau de alte tipuri de circumstanțe speciale, pe care le invocă serviciile de securitate, spre deosebire de organismele de supraveghere mai specializate, care au o experiență îndelungată în supravegherea acestor servicii.

În ultimul rând, însăși natura reclamațiilor împotriva serviciilor de informații poate face ca instanțele judecătorești convenționale sau organismele convenționale de reglementare să nu fie în măsură să le gestioneze. Reclamanții vor fi obligați adesea să încadreze reclamațiile concrete privind legalitatea sau probitatea conduitei astfel, încât acestea să corespundă unor motivații standard, civile sau de reglementare. Este posibil ca încadrarea să nu fie cea potrivită și reclamații care merită, altminteri, să fie luate în considerare pot fi respinse nu pentru că nu ridică semne reale de întrebare în raport cu serviciile de informații, ci pentru că aceste îndoieli nu pot fi formulate în limbajul jurisdicțional al organismului general care gestionează reclamații. De pildă, este posibil ca urmărirea ilegală a unei persoane să nu fie recunoscută ca delict civil în unele jurisdicții și, deci, să nu intre în sfera de competență a instanțelor judecătorești convenționale.

3.2 LOCURILE SPECIALIZATE

O reacție evidentă la aceste neajunsuri ale locurilor generale este crearea unor foruri mai specializate de gestionare a reclamațiilor. Locurile specializate se încadrează, în mod normal, într-una din următoarele trei categorii: întâi, pot fi poziţionate în interiorul ramurii executive (de exemplu, unii inspectori generali); în al doilea rând, pot fi independente față de executiv și parlament; și, în cele din urmă, pot fi organisme parlamentare.

3.2.1 Organismele interne de gestionare a reclamațiilor

Unele jurisdicții dispun de supraveghetori interni, prin intermediul cărora executivul politic controlează serviciile de informații. Astfel de organisme pot fi,

[30] Comisia de anchetă privind acțiunile oficialilor canadieni în cazul Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* [*Un nou mecanism de verificare a activităților RCMP legate de securitatea națională*] (2006), pp. 492–3 (disponibil la http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/eng/EnglishReportDec122006.pdf).

pur și simplu, un anumit minister sau un delegat special ministerial, denumit câteodată inspector general. Cu toate acestea, trebuie să se remarce că, în unele jurisdicții, inspectorul general este o entitate cu adevărat independentă – și anume, are siguranța menținerii în post și independență de acțiune, ceea ce îl plasează în afara comenzilor și controlului din partea executivului și a serviciilor de informații. În unele situații, organismele interne pot fi autorizate să primească reclamații publice.[31] Din perspectiva executivului, o asemenea abordare reduce nevoia de a dezvălui în afara unui cadru foarte restrâns informații clasificate, care pot fi de maximă relevanță într-o reclamație. În același timp, organismele interne de gestionare a reclamațiilor nu au independență și autonomie față de oficialii responsabili pentru serviciile de informații. Publicul poate să perceapă asemenea organisme ca fiind susceptibile de un conflict de interese – pe modelul „vulpii care păzește cotețul" – și poate să aibă îndoieli în privința legitimității unui proces intern de gestionare a reclamațiilor.

3.2.2 Organismele independente de gestionare a reclamațiilor

Structură

Existența unor organisme mai independente, și totuși strict specializate, de gestionare a reclamațiilor constituie un compromis evident între nevoia de a limita difuzarea informațiilor clasificate și aceea de a consolida legitimitatea publică. O serie de jurisdicții au înființat organisme specializate de supraveghere, independente din punct de vedere al personalului și al activităților în raport cu serviciile de informații și restul ramurii executive. Aceste agenții se bucură de credibilitate datorită faptului că funcționează în mod independent. Totuşi, ele pot fi suficient de apropiate de guvern în măsura în care membrii lor pot fi verificați din punct de vedere al securității și li se pot încredința informații clasificate. Exact o astfel de practică a fost codificată în legea ce reglementează unul dintre primele organisme de acest gen, SIRC din Canada, în eforturile de a tempera îngrijorarea serviciilor de informații cu privire la circulația informațiilor clasificate. Membrii SIRC sunt numiți de guvernul federal, dar numai după ce acesta se consultă cu partidele de opoziție din parlament. Ei se bucură de o siguranță considerabilă în privința menținerii în func-

[31] Consiliul Națiunilor Unite pentru Drepturile Omului, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum*, Paragraful 380 (despre competența ministrului ungar responsabil pentru primirea reclamațiilor privind activitățile agențiilor ungare de securitate); Paragrafele 521–523 (despre sistemul de control intern în Macedonia); și SUA, *Inspector General for the Central Intelligence Agency*, U.S. Code 50, §403q.

ţie, având un mandat de cinci ani, ce poate fi reînnoit, și își pot angaja staff propriu chiar dacă au nevoie de o aprobare din partea structurii guvernamentale responsabile cu gestiunea financiară. Fiecare membru depune un jurământ de păstrare a secretului și se supune legii canadiene privind secretele oficiale.[32]

În timp ce sistemul canadian nu obligă la numirea unor persoane cu expertiză specială, alte jurisdicții folosesc o abordare diferită. De exemplu, Comisia pentru reclamații privind serviciul de informații din Kenya este prezidată de un judecător și include alți patru membri, dintre care unul este un „avocat" cu nu mai puțin de șapte ani vechime, iar altul trebuie să fie un „conducător religios," „recunoscut pe plan național." Membrii comisiei sunt numiți de președinte, „la recomandarea Comisiei Serviciului Judiciar" și „vor deține funcția pe o perioadă de trei ani", putând fi numiți din nou, pentru cel mult două mandate.[33] La rândul său, Comisia I din Belgia este numită de Senat pentru un mandat de șase ani ce poate fi reînnoit, iar membrii săi trebuie să îndeplinească anumite criterii legate de cunoștințele juridice și experiența relevantă și nu pot fi membri ai unui serviciu de poliție ori de informații.[34]

Este dificil să se evalueze de la distanță buna credință a unor astfel de sisteme de numire independente. Totuși, principiul este unul temeinic. Mai mult, sistemele de numire care pretind competență și un istoric în profesie sunt garantate în măsura în care nu au ca efect crearea unei caste exclusiviste a persoanelor numite. Criteriile de numire prea stricte și exigente pot restrânge categoria persoanelor considerate a fi potrivite la cele care au un trecut în domeniul intelligence – o situație care ar duce la percepția (dacă nu chiar realitatea) că organismul de supraveghere a fost „acaparat" de serviciul de informații supus supravegherii.

Tribunalul cu Competențe de Investigare din Marea Britanie oferă exemplul unui set diferit de exigențe legate de profesie: stafful său e compus exclusiv din persoane care au deținut poziții înalte în sistemul judiciar sau au profesat

[32] Canadian Security Intelligence Service Act [Lege privind Serviciul Canadian pentru Informații de Securitate] (31 august 2004), R.S.C., Capitolul C-23, Secțiunile 35–37.

[33] Kenya, National Security Intelligence Service Act [Legea Serviciului Național pentru Informații de Securitate] (31 decembrie 1998), Secțiunea 25.

[34] Belgia, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment [Lege pentru reglementarea verificării poliției și serviciilor de informații și a Unității de Coordonare pentru Evaluarea Amenințărilor] (18 iulie 1991), Articolele 28 și 30.

ca juriști pe o perioadă de cel puțin 10 ani.[35] Totuși, o structură ce cuprinde numai juriști și foști judecători poate fi, la rândul ei, extremă. În cazul unui organism care serveşte un interes public general, angajarea personalului într-un mod ce reflectă o varietate de perspective și experiențe profesionale nu este lipsită de merite.

Este filozofia ce pare să anime SIRC din Canada: nu există cerințe profesionale preliminare pentru a face parte din această entitate. În schimb, membrii săi trebuie să fie membri ai Consiliului Privat din Canada, dar nu și ai forului legislativ federal în exercițiu. În practică, potențialii nominalizați provin din rândul foștilor politicieni de rang înalt, al celor mai importanți judecători și al unor persoane care s-au distins prin diverse merite ce îi califică pentru această onoare. Este întru totul posibil ca o persoană să fie numită în Consiliul Privat cu scopul principal de a deveni ulterior un membru al SIRC. Altfel spus, apartenența la SIRC este larg deschisă, permițând acestui organism (cel puțin în principiu) să reprezinte publicul larg pe care îl servește.

Însă, flexibilitatea abordării canadiene poate fi foarte greşită. Poate părea o ipocrizie ca un organism de gestionare a reclamațiilor, cu o funcție cvasi-judiciară, să fie alcătuit în întregime din membri fără pregătire juridică – o situație posibilă și actualmente reală în cazul SIRC din Canada. Oricare ar fi celelalte calități ale membrilor, absența pregătirii juridice poate crea dependență față de stafful de formație juridică al organismului respectiv. Este o situație care, la rândul ei, impune evaluarea atentă a carierei persoanelor din staff cu pregătire juridică și a traseului lor între organismele guvernamentale (incluzând, potențial, și serviciile de informații). Independența unui organism de gestionare a reclamațiilor poate fi prejudiciată (sau percepută ca atare) dacă membrii lui sunt dependenți de funcționarii publici de carieră, care pendulează în și în afara structurilor guvernamentale. Din această perspectivă, modelul ideal poate fi un organism de gestionare a reclamațiilor alcătuit din mai mulți membri, care să dispună de un staff cu experiențe profesionale diverse și în care un procent minim de membri să aibă, de exemplu, pregătire juridică.

Funcții

Unele jurisdicții au înființat organisme de supraveghere a căror unică funcție este aceea de a primi și investiga reclamații. De exemplu, în Marea Britanie, Tribunalul cu Competențe de Investigare „poate investiga reclamațiile referitoare la orice pretinsă conduită a sau în numele serviciilor de informații – Ser-

[35] Marea Britanie, website-ul Tribunalului cu Competențe de Investigare (disponibil la http://www.ipt-uk.com/default.asp?sectionID=1).

viciul de Securitate (denumit uneori MI5), Serviciul Secret de Informații (denumit uneori MI6) și GCHQ (Centrul de Comunicații al Guvernului).”[36]

În alte situații, funcția principală a unor asemenea organisme specializate este de a verifica performanțele serviciilor de informații, fie în mod independent, fie la cererea miniștrilor sau a parlamentarilor.[37] Cu toate acestea, entitățile respective pot fi, de asemenea, autorizate să primească (și să investigheze) reclamații privind serviciile de informații pe care, potrivit mandatului lor, le supraveghează.[38] De pildă, în Norvegia, Comisia parlamentară de supraveghere a serviciilor de informații este organismul ai cărui membri, deși sunt aleși de parlament, nu fac parte din punct de vedere instituțional din ramura legislativă. Pe lângă investigarea din proprie inițiativă a activităților serviciilor de informații, comisia poate să primească și să investigheze reclamații din partea publicului.[39] Și Comisia I din Belgia „se ocupă de reclamațiile și denunțurile pe care le primește cu privire la funcționarea, intervenția, acțiunea sau inacțiunea serviciilor de informații, Unității de Coordonare pentru Evaluarea Amenințărilor, precum și ale altor servicii de suport și ale personalului lor.”[40] Funcții si-

---

[36] Marea Britanie, website-ul Tribunalului cu Competențe de Investigare, „About IPT: What the Tribunal can investigate” [„Despre Tribunalul cu Competențe de Investigare: ce poate investiga Tribunalul”] (disponibil la: http://www.ipt-uk.com/sections.asp?sectionID=22&type=top).

[37] Olanda, Intelligence and Security Services Act [Lege privind serviciile de informații și de securitate], Articolele 64 și 78.

[38] Consiliul Națiunilor Unite pentru Drepturile Omului, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum*, Paragrafele 270 și 271 (despre funcțiile Consiliului pentru Supravegherea Civilă a Agențiilor de Informații de Securitate din Croația); Paragraful 279 (despre funcțiile Autorității Independente de Investigare a Alegațiilor și Reclamațiilor împotriva Poliției din Cipru); Paragraful 396 (despre funcțiile Comisiei de Ombudsman pentru Garda Siochána din Irlanda); Paragraful 410 (despre funcțiile Comisiei de Prefectură pentru Siguranța Publică din Japonia); Australia, Inspector-General of Intelligence and Security Act [Lege privind Inspectorul General pentru Informații și Securitate] (17 octombrie 1986), Secțiunea 8 (amendată).

[39] Consiliul Națiunilor Unite pentru Drepturile Omului, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum*, Paragraful 585; Norvegia, Act Relating to the Monitoring of Intelligence, Surveillance, and Security Services [Lege privind monitorizarea serviciilor de informații, supraveghere și securitate] (3 februarie 1995), Secțiunea 3 (disponibil la www.eos-utvalget.no/filestore/EOSAct.pdf).

[40] Belgia, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment [Lege pentru reglementarea verificării

milare sunt duse la îndeplinire în Africa de Sud de către Inspectorul General pentru Informații (IGI) – o entitate independentă în raport cu executivul și care răspunde în fața comisiei parlamentare de supraveghere menționate mai jos. Inspectorul general poate „primi și investiga reclamații ale unor membri ai publicului și ai serviciilor, conținând alegații referitoare la o administrare incorectă, un abuz de putere, încălcarea Constituției, a legilor și politicilor (privind informațiile și contrainformațiile), la corupție și îmbogățirea prin mijloace ilegale a oricărei persoane în urma unei acțiuni sau a lipsei de acțiune a unui membru.[41]

În unele jurisdicții, reclamațiile înaintate acestor organisme specializate de supraveghere trebuie să fie precedate de notificarea serviciului de informații în cauză. De exemplu, în Canada, o reclamație publică trebuie să fie adresată mai întâi directorului CSIS. Apoi, SIRC poate investiga reclamațiile serioase și făcute cu bună credință dacă directorul nu reacționează într-o perioadă de timp pe care comisia o consideră rezonabilă sau dacă oferă un răspuns necorespunzător.[42]

3.2.3 Organismele parlamentare de gestionare a reclamațiilor

O serie de jurisdicții dispun de organisme parlamentare speciale care supraveghează domeniul intelligence și serviciile aferente. Ca și în cazul unor organisme specializate de supraveghere menționate mai sus, aceste comisii parlamentare pot avea și sarcina de a primi și investiga reclamații referitoare la activitățile serviciilor de informații.[43] De exemplu, în Germania, Comisia speci-

poliției și serviciilor de informații și a Unității de Coordonare pentru Evaluarea Amenințărilor] (18 iulie 1991), Articolul 34.

41 Africa de Sud, Intelligence Services Oversight Act [Lege privind supravegherea serviciilor de informații] (23 noiembrie 1994), Secțiunea 7(7)(cA).

42 Canadian Security Intelligence Service Act [Lege privind Serviciul Canadian pentru Informații de Securitate] (31 august 2004), R.S.C., Capitolul C-23, Secțiunea 41.

43 Consiliul Națiunilor Unite pentru Drepturile Omului, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum*, Paragraful 270 (despre rolul Comisiei parlamentare pentru politică internă și securitate națională din Croația); Paragraful 380 (despre rolul Comisiei parlamentului ungar pentru securitate națională); și Paragrafele 609–611 (despre comisiile parlamentare comune din România, dar sugerând că vor investiga reclamații numai cu acordul altor comisii parlamentare); Larry Watts, „Control and Oversight of Security Intelligence in Romania" [„Controlul și supravegherea serviciilor de informații de securitate în România"], în *Democratic Control of Intelligence Services*, editori Hans Born și Marina Caparini (Aldershot, UK: Ashgate, 2007), p. 60 (despre reclamațiile examinate de comisiile parlamentare din România).

ală de control parlamentar poate examina reclamații.[44] În Africa de Sud, Comisia parlamentară mixtă permanentă pentru informații (un organism alcătuit din 15 parlamentari, care are funcția de a supraveghea serviciile de informații) nu investighează direct reclamațiile, dar poate:

> …ordona investigarea de către șeful serviciului ori de către Inspectorul General și primirea unui raport din partea acelorași cu privire la orice reclamație primită de comisie din partea oricărui individ, care se referă la ceva considerat de acesta că i-a afectat persoana sau proprietatea și care a fost provocat de un serviciu, cu condiția ca reclamația în cauză să nu fie considerată de comisie lipsită de importanță sau jignitoare, ori făcută cu rea-credință.[45]

Mandatarea comisiilor parlamentare atât cu funcția de supraveghere, cât și cu cea de gestionare a reclamațiilor permite concentrarea expertizei referitoare la sectorul de securitate într-un singur organism și, în același timp, limitează diseminarea informațiilor clasificate. Există, totuși, o serie de neajunsuri care decurg din mandatarea organismelor parlamentare de supraveghere cu funcția de gestionare a reclamațiilor. În primul rând, este posibil ca parlamentarii să nu aibă suficientă expertiză sau timpul necesar pentru a investiga reclamațiile și a decide cu privire la acestea. În al doilea rând, parlamentarii sunt, prin definiție, actori partizani. Ceea ce poate compromite capacitatea lor de a investiga și de a judeca în mod corespunzător reclamațiile care ridică probleme deosebit de sensibile cu privire la conduita guvernelor în exercițiu. În al treilea rând, gestionarea reclamațiilor poate impune examinarea atentă a detaliilor, reguli pentru asigurarea corectitudinii procedurale, evaluări pe bază de probe legate, de exemplu, de credibilitatea martorilor, care sunt gestionate mai bine într-un mediu mai apropiat de cel judiciar. În fine, comisiile parlamentare au deseori un număr mare de membri, ceea ce îngreunează procesul de stabilire a concluziilor și de formulare a acestora cu claritate.

4. PROCEDURILE DE GESTIONARE A RECLAMAȚIILOR ȘI CONTROLUL INFORMAȚIILOR

În acest scurt capitol, nu este posibilă descrierea detaliată a procedurilor de gestionare a reclamațiilor. În consecință, accentul va fi pus pe câteva conside-

[44] DCAF, Backgrounder: Parliamentary Oversight of Intelligence Services [Document informativ: Supravegherea parlamentară a serviciilor de informații] (2006) (notând că, în Germania, Comisia specială de control parlamentar poate examina reclamațiile cetățenilor); Germania, Control Panel Act [Lege privind Comisia specială de control] (29 iulie 2009), în *Federal Law Gazette I*, p. 2346, Secțiunea 8.

[45] Africa de Sud, Intelligence Services Oversight Act [Lege privind supravegherea serviciilor de informații] (23 noiembrie 1994), Secțiunea 3(1)(f).

rente procedurale generale, precum și pe procedurile utilizate pentru protecția informațiilor clasificate. Dat fiind că procedurile folosite de organismele cu mandate mai generale (adică mandate care depășesc sfera serviciilor de informații) variază foarte mult, accentul este pus în această secțiune pe procedurile aplicate de organismele specializate (în domeniul intelligence și al securității naționale) de gestionare a reclamațiilor (CHB) despre care s-a discutat în secțiunea 3.2 de mai sus.

4.1 REGULI PROCEDURALE GENERALE

Legislația de reglementare din unele jurisdicții prevede că reclamațiile trebuie făcute în scris.[46] CHB pot fi autorizate să respingă reclamațiile considerate a fi lipsite de importanță, jignitoare, făcute cu rea-credință sau care, într-un fel sau altul, se situează sub un prag *de minimis*, necesar pentru declanșarea unei investigații.[47] O asemenea restricție limitează, în mod evident, efectul regulilor referitoare la caracterul general al motivației, permițând organismului să respingă pur și simplu reclamații considerate a nu avea merite. Desigur, dacă sunt aplicate prea des, pentru a evita cazurile dificile, asemenea reguli vor face ca organismul să devină ineficient în îndeplinirea funcțiilor sale de supraveghere și de gestionare a reclamațiilor. În cele din urmă, măsura de siguranță pentru folosirea corectă a acestor reguli de filtrare rezidă în însăși independența organismului respectiv. Dacă are un staff corespunzător, format din persoane atente, calificate și suficient de autonome în raport cu guvernul, vor exista puține motive pentru a renunța, din presupuse rațiuni procedurale, la cazurile controversate.

[46] Australia, Inspector-General of Intelligence and Security Act [Lege privind Inspectorul General pentru Informații și Securitate] (17 octombrie 1986), Secțiunea 10 (amendată); Noua Zeelandă, Inspector-General of Intelligence and Security Act [Lege privind Inspectorul General pentru Informații și Securitate] (1 iulie 1996), Secțiunea 16.

[47] Australia, Inspector-General of Intelligence and Security Act [Lege privind Inspectorul General pentru Informații și Securitate] (17 octombrie 1986), Secțiunea 11 (amendată); Africa de Sud, Intelligence Services Oversight Act [Lege privind supravegherea serviciilor de informații] (23 noiembrie 1994), Secțiunea 3(1)(f); Noua Zeelandă, Inspector-General of Intelligence and Security Act [Lege privind Inspectorul General pentru Informații și Securitate] (1 iulie 1996), Secțiunea 17; Belgia, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment [Lege pentru reglementarea verificării poliției și serviciilor de informații și a Unității de Coordonare pentru Evaluarea Amenințărilor] (18 iulie 1991), Articolul 34.

Este foarte important ca CBH să nu confunde reclamațiile „lipsite de importanță și jignitoare” cu cele care „nu sunt însoțite de suficiente detalii.” După cum s-a remarcat deja, reclamațiile împotriva conduitei unui serviciu de informații cu activitate clandestină și secretă pot duce lipsă, în mod firesc, de un număr mare de detalii, care se asociază, de regulă, unor activităţi mai transparente. De asemenea, respingerea întemeiată pe „rea-credință” nu trebuie utilizată pur și simplu ca reacție în cazul unor reclamanți dificili. Înaintarea unei reclamații împotriva unui serviciu de informații puternic reprezintă o perspectivă ce intimidează și, mai curând, descurajează reclamanții, cu excepția celor mai încăpățânați. Reclamanții – și în special informatorii interni – pot manifesta particularități de comportament care îi determină pe observatori să pună la îndoială legitimitatea reclamației lor. Trebuie făcută cu grijă distincția între fapte și trăsăturile de personalitate care pot genera îndoieli în privința credibilității.

În cazul organizării unor audieri sau al desfășurării unor anchete, regulile care guvernează activitatea CHB, cel puțin a unora dintre ele, impun standarde de corectitudine procedurală, cerând, de pildă, ca părțile afectate să fie audiate înainte de a se face constatări ce pun sub semnul întrebării conduita acestor persoane.[48]

4.2 COMPETENȚELE ORGANISMELOR DE GESTIONARE A RECLAMAȚIILOR

Unele CHB au puterea de a obliga la prezentarea unor documente și la prezența martorilor.[49] E posibil ca, în unele situații, astfel de puteri să fie foarte extinse și să prevaleze asupra unor concepte precum privilegiul avocat – cli-

---

48 Australia, Inspector-General of Intelligence and Security Act [Lege privind Inspectorul General pentru Informații și Securitate] (17 octombrie 1986), Secțiunea 19 (amendată).

49 Australia, Inspector-General of Intelligence and Security Act [Lege privind Inspectorul General pentru Informații și Securitate] (17 octombrie 1986), Secțiunea 18 (amendată); Norvegia, Act Relating to the Monitoring of Intelligence, Surveillance, and Security Services [Lege privind monitorizarea serviciilor de informații, supraveghere și securitate] (3 februarie 1995), Secțiunile 4 și 5; Germania, Control Panel Act [Lege privind Comisia specială de control] (29 iulie 2009), în *Federal Law Gazette I*, p. 2346, Secțiunea 5; Noua Zeelandă, Inspector-General of Intelligence and Security Act [Lege privind Inspectorul General pentru Informații și Securitate] (1 iulie 1996), Secțiunile 20 și 23; Kenya, National Security Intelligence Service Act [Legea Serviciului Național pentru Informații de Securitate] (31 decembrie 1998), Secțiunea 26; Belgia, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment [Lege pentru reglementarea verificării poliției și serviciilor de informații și a Unității de Coordonare pentru Evaluarea Amenințărilor] (18 iulie 1991), Articolul 48.

ent.[50] De exemplu, SIRC poate avea acces la toate informațiile aflate în posesia serviciului de informații, excluzând discuțiile confidențiale ale Cabinetului (în esență, înregistrările dezbaterilor din ședințele de Cabinet). Într-o altă situație, în SUA, Inspectorul General al CIA

> … va avea acces la orice angajat al Agenției, sau la orice angajat al unui contractor al Agenției, a cărui mărturie este necesară pentru a-și îndeplini îndatoririle. În plus, va avea acces direct la toate înregistrările … care au legătură cu programele și operațiunile în privința cărora responsabilitatea îi revine Inspectorului General … Refuzul oricărui angajat sau contractor de a coopera cu Inspectorul General va constitui un temei pentru acțiuni administrative corespunzătoare din partea Directorului, inclusiv pierderea locului de muncă sau încetarea relației contractuale existente.[51]

Pentru alte CHB, accesul la informații este mai limitat. În Africa de Sud, legislația de reglementare îi interzice Comisiei parlamentare mixte permanente pentru informații accesul la informații care ar putea dezvălui identitatea informatorilor serviciilor de informații.[52] (Pe de altă parte, IGI din Africa de Sud își desfășoară activitatea cu mai puține restricții – nicio formă de acces la informații, date sau incinte (ale serviciului de securitate) nu poate fi refuzată inspectorului general „sub niciun temei."[53]) Limitarea accesului la informații secrete al unui organism pentru gestionarea reclamațiilor reprezintă un efort clar de diminuare a scurgerilor voluntare sau involuntare de informații. Cu toate acestea, limitările pot afecta capacitatea organismului respectiv de a evalua în detaliu importanța reclamațiilor. Altfel spus, pot constitui un handicap pentru CHB de la bun început. Ceea ce este, așadar, un motiv de preocupare în situația în care se intenționează crearea unui CHB care să aibă un rol semnificativ.

O soluție parțială pentru problema dificilă a securității informațiilor este specificarea în regulile care guvernează CHB a cerințelor ce trebuie respectate în

---

50 Australia, Inspector-General of Intelligence and Security Act [Lege privind Inspectorul General pentru Informații și Securitate] (17 octombrie 1986), Secțiunea 18 (amendată).

51 SUA, Inspector General for the Central Intelligence Agency [Inspectorul General pentru Agenția Centrală de Informații], U.S. Code 50, §403q (e)(2). A se vedea și paragrafele (4) și (5).

52 Africa de Sud, Intelligence Services Oversight Act [Lege privind supravegherea serviciilor de informații] (23 noiembrie 1994), Secțiunea 5.

53 Africa de Sud, Intelligence Services Oversight Act [Lege privind supravegherea serviciilor de informații] (23 noiembrie 1994), Secțiunea 7.

gestionarea informațiilor.[54] De pildă, IGI sud-african trebuie „să respecte toate cerințele referitoare la securitate aplicabile angajaților din serviciile de informații."[55] În Canada, membrii SIRC sunt obligați să respecte legea canadiană privind secretele oficiale și, deci, pot fi puși sub urmărire penală dacă dezvăluie din greșeală informații secrete.[56]

Există și protocoale pentru a controla fluxul concret de informații. De exemplu, cercetătorii SIRC verifică, de regulă, informațiile clasificate în birourile securizate ale SIRC din sediul CSIS. Există, însă, unele situații în care informațiile sunt mutate în propriile amplasamente securizate ale SIRC, cu precădere în cazurile în care informațiile respective sunt de maximă relevanță pentru reclamațiile examinate de SIRC. Crearea acestei infrastructuri pentru gestionarea informațiilor poate impune o investiție substanțială, iar într-o țară de mari dimensiuni din punct de vedere geografic (precum Canada) poate limita locurile în care SIRC își va desfășura activitatea.

4.3 CONFIDENȚIALITATEA DIN RAȚIUNI DE SECURITATE NAȚIONALĂ

După cum sugerează cele de mai sus, gestionarea cu profesionalism a informațiilor legate de securitatea națională este o preocupare fundamentală în orice sistem de gestionare a reclamațiilor. Legislația de reglementare, în cazul unui număr semnificativ de CHB, precizează că anchetele și/sau audierile trebuie să se desfășoare în condiții de confidențialitate.[57] În plus, constatările făcute de CHB pot fi editate și/sau diseminarea lor poate fi restricționată. De

[54] Africa de Sud, Intelligence Services Oversight Act [Lege privind supravegherea serviciilor de informații] (23 noiembrie 1994), Secțiunea 7; Germania, Control Panel Act [Lege privind Comisia specială de control] (29 iulie 2009), în *Federal Law Gazette I*, p. 2346, Secțiunea 10.

[55] Africa de Sud, Intelligence Services Oversight Act [Lege privind supravegherea serviciilor de informații] (23 noiembrie 1994), Secțiunea 7; a se vedea limitări similare în Norvegia, Act Relating to the Monitoring of Intelligence, Surveillance, and Security Services [Lege privind monitorizarea serviciilor de informații, supraveghere și securitate] (3 februarie 1995), Secțiunea 9; Noua Zeelandă, Inspector-General of Intelligence and Security Act [Lege privind Inspectorul General pentru Informații și Securitate] (1 iulie 1996), Secțiunea 13.

[56] Canada, Security of Information Act [Lege privind siguranța informațiilor] (1985), R.S.C., Capitolul O-5, anexă.

[57] Australia, Inspector-General of Intelligence and Security Act [Lege privind Inspectorul General pentru Informații și Securitate] (17 octombrie 1986), Secțiunea 17 (amendată); Noua Zeelandă, Inspector-General of Intelligence and Security Act [Lege privind Inspectorul General pentru Informații și Securitate] (1 iulie 1996), Secțiunea 19; Kenya, National Security Intelligence Service Act [Legea Serviciului Național pentru Informații de Securitate] (31 decembrie 1998), Secțiunea 26.

exemplu, în Australia, IGIS nu trebuie să comunice reclamantului constatările făcute decât „după ce șeful agenției (de informații) relevante și Inspectorul General au ajuns la concluzia că răspunsul dat reclamantului, în termenii propuși, nu va prejudicia securitatea, apărarea Australiei sau relațiile Australiei cu alte țări.”[58] Nici în Africa de Sud, IGI nu poate dezvălui informațiile restricționate fără permisiunea prealabilă a guvernului.[59] În mod asemănător, în Kenya, Comisia pentru reclamații trebuie „să țină seama de cerințele de securitate națională” în îndeplinirea funcțiilor sale. În acest scop, trebuie să se consulte cu directorul general al Serviciului pentru Informații de Securitate Națională (iar la nivel ministerial, cu Consiliul pentru Securitate Națională), „pentru a stabili informațiile sau circumstanțele în care anumite informații nu pot fi dezvăluite pe parcursul niciunei anchete, sau în legătură cu aceasta, în interesul securității naționale.”[60] În Norvegia, declarațiile comisiei, adresate reclamanților „trebuie să fie cât mai complete posibil, fără a dezvălui informații clasificate.”[61]

Deoarece caracterul secret poate afecta capacitatea reclamantului de a avea câștig de cauză, unele jurisdicții pot întrebuința proceduri speciale, stabilind ca anumite segmente ale audierilor să aibă loc cu ușile închise, pentru veni în sprijinul reclamantului. În Canada, de exemplu, juriștii SIRC au sarcina de

> … a contesta în instanță deciziile privind nedezvăluirea informațiilor conținute în materialul confidențial, precum și de a interoga martorii guvernamentali în ședințe cu ușile închise…. Pot fi angajați juriști din exterior (sau „agenți juridici”) în situațiile în care, din cauza volumului mare de muncă, juriștii interni nu sunt pe deplin capabili să acționeze în cadrul litigiilor din instanță. În alte situații, pot

[58] Australia, Inspector-General of Intelligence and Security Act [Lege privind Inspectorul General pentru Informații și Securitate] (17 octombrie 1986), Secțiunea 23 (amendată).

[59] Africa de Sud, Intelligence Services Oversight Act [Lege privind supravegherea serviciilor de informații] (23 noiembrie 1994), Secțiunea 5.

[60] Kenya, National Security Intelligence Service Act [Legea Serviciului Național pentru Informații de Securitate] (31 decembrie 1998), Secțiunea 26.

[61] Norvegia, Instructions for Monitoring of Intelligence, Surveillance and Security Services (EOS) [Instrucțiuni pentru monitorizarea serviciilor de informații, supraveghere și securitate (EOS)] emise în baza Secțiunii 1 din Act No. 7 of 3 February 1995 relating to the Monitoring of Intelligence, Surveillance and Security Services [Legea nr. 7 din 3 februarie 1995 privind monitorizarea serviciilor de informații, supraveghere și securitate], Secțiunea 8; a se vedea și Noua Zeelandă, Inspector-General of Intelligence and Security Act [Lege privind Inspectorul General pentru Informații și Securitate] (1 iulie 1996), Secțiunea 25.

fi angajați agenți juridici atunci când juriștii interni consideră că speța respectivă va necesita o interogare deosebit de agresivă a părții adverse CSIS.[62]

5. REMEDII

Așa cum s-a remarcat mai înainte, scopul principal al oricărui sistem de reclamații este „remediul efectiv." De notat că remediile acordate de organismele de gestionare a reclamațiilor împotriva serviciilor de informații se constituie frecvent în recomandări, și mai puțin în decizii juridice obligatorii cu privire, de pildă, la acordarea de despăgubiri.[63] Aceste puteri limitate reflectă, probabil, dualitatea mandatului unui număr mare de CHB, și anume organismul care examinează reclamațiile este unul și același cu organismul care efectuează supravegherea autonomă a activităților serviciilor de informații. Aceste procese de supraveghere generează, de regulă, recomandări la adresa serviciului de informații în cauză și la adresa executivului, cu privire la reformarea politicilor și practicilor. Acolo unde supravegherea reprezintă funcția principală

---

[62] Craig Forcese și Lorne Waldman, „Seeking Justice in an Unfair Process: Lessons from Canada, the United Kingdom, and New Zealand on the Use of 'Special Advocates' in National Security Proceedings" [„Căutarea dreptății într-un proces incorect: lecții din Canada, Marea Britanie și Noua Zeelandă privind folosirea «avocaților speciali» în proceduri judiciare vizând securitatea națională"] (studiu comandat de Centrul Canadian pentru Studii de Informații și Securitate, cu sprijinul financiar al Serviciului Administrativ al Tribunalelor) (august 2007), pp. 7–8.

[63] Canadian Security Intelligence Service Act [Lege privind Serviciul Canadian pentru de Informații de Securitate] (31 august 2004), R.S.C., Capitolul C-23, Secțiunea 52 (despre competențele SIRC); Olanda, Intelligence and Security Services Act [Lege privind serviciile de informații și de securitate], Articolul 84 (despre competențele Ombudsmanului Național); Consiliul Națiunilor Unite pentru Drepturile Omului, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum*, Paragraful 77 (despre competențele Comisarului pentru viață privată din Belgia); și Paragraful 585 (despre competențele comisiei de supraveghere din Norvegia); Australia, Inspector-General of Intelligence and Security Act [Lege privind Inspectorul General pentru Informații și Securitate] (17 octombrie 1986), Secțiunea 24 (amendată); Norvegia, Instructions for Monitoring of Intelligence, Surveillance and Security Services (EOS) [Instrucțiuni pentru monitorizarea serviciilor de informații, supraveghere și securitate (EOS)] emise în baza Secțiunii 1 din Act No. 7 of 3 February 1995 relating to the Monitoring of Intelligence, Surveillance and Security Services [Legea nr. 7 din 3 februarie 1995 privind monitorizarea serviciilor de informații, supraveghere și securitate], Secțiunea 8; Noua Zeelandă, Inspector-General of Intelligence and Security Act [Lege privind Inspectorul General pentru Informații și Securitate] (1 iulie 1996), Secțiunea 25; Kenya, National Security Intelligence Service Act [Legea Serviciului Național pentru de Informații de Securitate] (31 decembrie 1998), Secțiunea 26.

a CHB, legiuitorii, care au înființat aceste instituții, au considerat, probabil, că acordarea unor competențe coercitive de compensare, ca răspuns la reclamații, este incompatibilă cu atributele mai puțin adversative, necesare unei supravegheri eficace.

Totuși, în practică, a limita rolul CHB la recomandări poate însemna diminuarea capacității lor de a face mai mult decât să pretindă unui serviciu de informații să se conformeze. O astfel de abordare poate fi deosebit de dificilă acolo unde rezultatele investigării unor reclamații sunt ele însele clasificate, o practică frecventă, menționată mai sus. Din acest motiv, e meritoriu faptul că organismele CHB furnizează versiuni editate ale constatărilor lor în cadrul rapoartelor anuale disponibile public sau sub alte forme. Totuși, chiar și acestea pot atrage surprinzător de puțină atenție din partea parlamentarilor și a mass-mediei. De pildă, SIRC din Canada a publicat în rezumat constatări, uneori incriminatoare, care au stârnit un slab interes.

În cele mai rele situații, o competență care se limitează la a recomanda poate avea ca efect diminuarea oricăror alte merite ale CHB. Dacă potențialii reclamanți se îndoiesc că acțiunile lor vor avea ca rezultat un răspuns, o schimbare sau o compensație semnificative, atunci vor avea puține motive să înainteze o reclamație la CHB. În consecință, reclamanții vor încerca să-și înainteze reclamațiile pe alte canale (precum instanțele generale, care nu sunt în situația de a le gestiona în mod corespunzător), să le aducă la cunoștința mass-mediei în speranța de a stârni o reacție, sau, pur și simplu, să renunțe la acest efort. Toate reacțiile de mai sus subminează rațiunea de a fi a organismelor CHB – aceea de a dezvălui delictele comise de serviciile de informații și de a reacționa la acestea.

Alte organisme dispun de competențe care seamănă mai mult cu cele „judiciare.” Ceea ce este adevărat în special în cazul CHB care se ocupă exclusiv de gestionarea reclamațiilor. Astfel, organisme cvasi-judiciare, precum Tribunalul cu Competențe de Investigare din Marea Britanie, au puterea să impună „... măsuri reparatorii, precum anularea oricăror mandate, distrugerea oricăror înregistrări deținute sau compensarea financiară.”[64]

---

[64] Marea Britanie, website-ul Tribunalului cu Competențe de Investigare, „Complaints process: What happens to my complaint?” [„Procedura reclamațiilor: ce se întâmplă cu reclamația mea ?”] (http://www.ipt-uk.com/sections.asp?sectionID=4&chapter=0&type=top); Marea Britanie, Regulation of Investigatory Powers Act [Lege privind reglementarea competențelor de investigare], 2000, Capitolul 23, Secțiunea 67.

6. RECOMANDĂRI

Din studiul de față, referitor la organismele de gestionare a reclamațiilor, reies mai multe recomandări. Acestea sunt rezumate în rândurile următoare și sunt propuse ca „cele mai bune practici" în Tabelul 1.

- Statele trebuie să înființeze organisme de gestionare a reclamațiilor mandatate să primească și să investigheze atât reclamațiile din interior, cât și pe cele publice.

Sistemele de gestionare a reclamațiilor din interior constituie un mijloc de dirijare a denunțurilor interne printr-un cadru instituțional, care reacționează la reclamațiile ce merită atenție și poate răspunde preocupării guvernului privind protecția informațiilor clasificate. Totuși, acest sistem trebuie să-și extindă protecția și asupra celor care apelează la el.

- Un sistem eficace pentru reclamații din interior trebuie să includă garanții privind nerecurgerea la represalii atunci când angajații înaintează cu bună credință reclamații organismelor autorizate.

Prin comparație, sistemele pentru reclamații publice sunt mai extinse și, în general, se află la dispoziția tuturor. Câteva jurisdicții impun condiții legate de naționalitate, deși, în general, acestea se aplică numai în raport cu operațiunile serviciilor de informații externe; și chiar mai puține sunt jurisdicțiile care impun condiția ca reclamantul să fie personal afectat, într-un fel sau altul, de aspectele semnalate în reclamație. Este dificil de apreciat care sunt meritele reale ale unor asemenea limitări.

- Organismele de gestionare a reclamațiilor trebuie să dispună de competențe extinse pentru primirea plângerilor din partea populației.

Dacă regulile referitoare la persoanele în măsură să înainteze reclamații au un caracter general, va crește numărul reclamațiilor ce pot fi înaintate organismului de gestionare a acestora. Asemenea reguli sporesc și potențialele sarcini ce revin respectivei entități. Ar putea fi mai potrivit să se limiteze aceste cazuri la cele care merită să fie luate în considerare. Însă trebuie acordată atenție modului în care se face o asemenea evaluare.

- Preocuparea față de plângerile lipsite de importanță sau jignitoare poate fi rezolvată prin reguli ce permit organismului de gestionare a reclamațiilor să elimine astfel de plângeri din fazele timpurii ale procesului. Dar trebuie să se acționeze cu grijă pentru a se evita respingerea reclamațiilor dificile, controversate din punct de vedere politic sau care, pur și simplu, sunt înaintate de persoane dificile.

Din punct de vedere al locului în care pot fi adresate, statele trebuie să analizeze cu atenție dacă instanțele judecătorești generale sau organismele

convenționale de reglementare sunt dotate adecvat pentru a se ocupa de reclamațiile împotriva serviciilor de informații. În practică, este posibil ca asemenea organisme să nu fie în măsură să gestioneze materiale și/sau informații clasificate vizând securitatea națională, rezultatul fiind acela că eficacitatea lor va fi afectată și nu vor avea capacitatea să investigheze reclamațiile respective în mod corespunzător. În plus, se poate ca organismele generale să nu dispună de expertiză în materie, necesară pentru o investigare amănunțită a acestor chestiuni.

Prin comparație, organismele specializate în gestionarea reclamațiilor din domeniul intelligence pot fi structurate astfel, încât să răspundă preocupărilor privind protecția informațiilor clasificate. În același timp, aceste preocupări legate de caracterul secret nu trebuie să aibă ca efect diminuarea funcțiilor organismului specializat până la punctul în care credibilitatea sa, ca organism de gestionare a reclamațiilor, se evaporă. Transparența trebuie să fie regula, iar caracterul secret trebuie limitat la circumstanțele ce ţin de buna credinţă. Mai mult, trebuie să se depună eforturi pentru a se asigura un oarecare echilibru între capacitatea guvernului și cea a reclamanților de a-și susține cazurile. Acolo unde guvernul își poate camufla poziția prin secretizare, organismul însuși trebuie să fie sigur că examinează cazul într-o manieră inchizitorială. În plus, membrii organismului de supraveghere trebuie să aibă, ei înșiși, certificate de securitate și un acces extins la informațiile aflate în posesia guvernului și a serviciilor de informații.

- În cele mai multe situații, organismele specializate de gestionare a reclamațiilor sunt de preferat organismelor mai generale atunci când se investighează reclamații împotriva serviciilor de informații. Acestor organisme trebuie să li se acorde puteri foarte extinse de acces la informațiile clasificate și trebuie să li se ceară să implementeze măsuri de siguranță pentru a reduce riscul scurgerii (voluntare sau involuntare) de informații. Exemple ale unor astfel de măsuri de siguranță pot fi protocoalele speciale de gestionare a informațiilor și obligația de a obține certificate de securitate.

În plus, organismele de gestionare a reclamațiilor vor fi credibile numai dacă își angajează stafful și funcționează în mod independent în raport cu guvernul și dacă dispun de resurse adecvate. Chiar dacă aceste organisme nu trebuie să fie alcătuite exclusiv din persoane cu o anumită pregătire profesională (de exemplu, juriști), în componența lor trebuie să se regăsească, într-o proporție adecvată, și reprezentanți cu pregătire juridică. Competența juridică independentă diminuează ceea ce ar putea fi altminteri o dependență excesivă de per-

soane din staff de formație juridică (și care, poate, nu sunt întru totul independente).

- Organismele de gestionare a reclamațiilor trebuie să fie independente față de guvern. Ceea ce, în practică, înseamnă că nu sunt numite unilateral de către guvernele în exercițiu și că au libertatea de a funcționa autonom în raport cu guvernul, membrii lor bucurându-se, totodată, de siguranța menținerii în funcție. Cel puțin o parte din membri trebuie să aibă pregătire juridică pentru a evita dependența excesivă de personalul serviciilor de informații atunci când examinează reclamațiile.

În sistemele de gestionare a reclamațiilor, problema remediilor este cea mai dificilă. În general, organismele cu cea mai mare putere de a acorda compensații pentru greșelile comise de serviciile de informații (instanțele judecătorești) sunt cel mai puțin dotate pentru a se ocupa de reclamațiile care au legătură cu circumstanțele speciale în care activează serviciile de informații, îndeosebi cerințele de secretizare și de protejare a informațiilor clasificate. Adeseori, organismele specializate de supraveghere sunt mai bine dotate pentru a risipi ceața produsă de secretizare, însă, în general, puterea lor se limitează la a face recomandări. Statele ar trebui să analizeze cu atenție posibilitatea ca organismele specializate de supraveghere, învestite cu funcții de gestionare a reclamațiilor, să aibă și competențe cvasi-judiciare de acordare a unor măsuri reparatorii, așa cum ar fi puterea de a acorda o compensație financiară persoanelor care au fost nedreptățite.

- Dotarea organismelor de gestionare a reclamațiilor numai cu puteri de recomandare e insuficientă și nu reprezintă un „remediu efectiv.” Mai degrabă, ar trebui să li se acorde acestor organisme competențe cvasi-judiciare, precum puterea de a acorda compensații financiare.

În fine, statele trebuie să evite dependența exclusivă de un model bazat pe reclamații pentru a asigura tragerea la răspundere a serviciilor de informații. Gestionarea reclamațiilor are locul său în acest proces; totuși, experiența unor state care se bazează exclusiv pe astfel de organisme pentru a îndeplini această funcție nu a fost una pozitivă. În Canada, de pildă, funcțiile în materie de securitate națională, exercitate de poliția federală (RCMP), sunt supuse numai unui mecanism modest de tragere la răspundere, bazat pe reclamații. O anchetă judiciară cu privire la practicile îndoielnice ale RCMP de combatere a terorismului, în urma evenimentelor din 11 septembrie 2001, a recomandat atât puteri sporite de gestionare a reclamațiilor, cât și un sistem de verificare bazat pe auditarea performanței. Ancheta a conchis că „... nevoia unor verificări din proprie inițiativă decurge din faptul că cele mai multe activități ale RCMP privind securitatea națională se desfășoară în secret și se supun unei

examinări judiciare insuficiente, dacă există vreuna, dar sunt potențial capabile să afecteze serios drepturile și libertățile individuale."[65]

O perspectivă îngustă, care pune accentul pe modelele de tragere la răspundere bazate pe reclamații, riscă să creeze o formă „teatrală" a răspunderii: existența organismului creează aparența unei separări a puterilor, însă el nu poate funcționa efectiv din cauza secretului care înconjoară activitatea serviciilor de informații. Această secretizare poate face ca persoanele ce constituie ținte ale serviciilor de informații să ignore, de pildă, încălcarea neautorizată a dreptului lor la viață privată. Din acest motiv, sistemele de gestionare a reclamațiilor care nu sunt însoțite de alte forme de verificare și supraveghere, în măsură să expună fapte reprobabile, constituie o abordare mediocră a guvernanței în domeniul intelligence.

- Dependența exclusivă de un model de tragere la răspundere a serviciilor de informații bazat pe reclamaţii nu este oportună. O astfel de abordare trebuie completată cu un sistem de verificare și/sau supraveghere independentă.

---

[65] Comisia de anchetă asupra acțiunilor oficialilor canadieni în cazul Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* [*Un nou mecanism de verificare a activităților RCMP legate de securitatea națională*] (2006), p. 18.

TABELUL 1. LISTA CELOR MAI BUNE PRACTICI DE GESTIONARE A RECLAMAȚIILOR	
Practica	**Implicații ale nerespectării practicii**
Este CHB dotat adecvat din punct de vedere al domeniului de competență și al expertizei juridice ?	Dacă nu, poate fi pusă sub semnul întrebării capacitatea CHB de a examina reclamațiile într-o manieră eficace și credibilă.
Are CHB acces deplin la informațiile secrete ale serviciului de informații ?	Dacă nu, CHB riscă să nu aibă efectiv capacitatea de a stabili valoarea reclamațiilor și de a evalua conduita serviciului.
Este CHB independent față de guvern și de serviciul de informații în ceea ce privește procesul de numire, siguranța postului și conducerea operațiunilor ?	Dacă nu, CHB va fi, probabil, lipsit de credibilitate și este posibil ca, în fapt, să nu poată lua decizii independente.
Primește CHB atât reclamații din interior, cât și reclamații publice ?	Dacă nu, reclamanții din interior pot fi împinși să recurgă la dezvăluiri, de pildă, în mass-media, iar celorlalte persoane le rămâne opțiunea să-și înainteze reclamațiile instanțelor judecătorești generale sau altor organisme care sunt slab dotate pentru a se pronunța asupra unor chestiuni de securitate națională.
Atunci când fac reclamații cu bună credință, sunt reclamanții din interior protejați împotriva represaliilor, în temeiul legii de angajare și/sau în temeiul legii privind secretele oficiale ?	Dacă nu, reclamanții din interior nu vor fi stimulați să parcurgă procesul CHB sau, pur și simplu, vor fi total descurajați să dezvăluie delictele.
Este jurisdicția asupra reclamațiilor publice formulată suficient de general pentru a permite oricăror persoane să înainteze reclamații care să vizeze întreaga gamă de activități ale serviciului de informații ?	Dacă nu, preocupările legitime legate de conduita serviciului de informații pot rămâne neobservate.
Dacă dispune de competența de a elimina reclamațiile ce nu merită atenție, are CHB grijă să-și exercite această putere cu prudență și fără a ține seama de considerente neesențiale, precum implicațiile politice ale reclamației sau calitățile irelevante ale reclamantului ?	Dacă nu, preocupările legitime privind conduita serviciului de informații pot fi eliminate prea ușor.
Are CHB puterea de a stabili remedii cvasi-judiciare, precum compensația financiară ?	Dacă nu, constatările CHB pot avea un impact scăzut asupra conduitei serviciului de informații, iar reclamanții pot fi descurajați de la bun început să facă reclamații.

Lista contributorilor

HANS BORN este cercetător principal la DCAF. În prezent, se ocupă cu precădere de problematica supravegherii serviciilor de informaţii, precum și a rolului parlamentelor și instituțiilor de tip ombudsman în guvernanța sectorului de securitate. Specializarea sa regională este Asia de Sud-Est (inclusiv Cambodgia, Indonezia, Filipine și Thailanda). A elaborat studii în domeniile drepturilor omului, responsabilității și guvernanței sectorului de securitate, pentru Națiunile Unite, Organizația pentru Securitate și Cooperare în Europa, Consiliul Europei și Parlamentul European. A fost co-inițiatorul Forumului Interparlamentar pentru guvernanța sectorului de securitate în Asia de Sud-Est (www.ipf-ssg-sea.net) și al Conferinței Internaționale pentru instituțiile de tip ombudsman pentru forțele armate (www.icoaf.org). A publicat numeroase lucrări despre reforma și guvernanța sectorului de securitate. Ultimele sale publicații includ: *Governing the Bomb: Democratic accountability and civilian control of nuclear weapons* [Controlând bomba: responsabilitatea democratică și controlul civil asupra armelor nucleare] (Oxford University Press, 2011), *Accountability of International Intelligence Cooperation* [Responsabilitatea cooperării internaționale în domeniul intelligence] (Routledge 2011) și *Parliamentary Oversight of the Security Sector: ECOWAS Parliament-DCAF Guide for West African Parliamentarians* [Supravegherea parlamentară a sectorului de securitate: Parlamentul ECOWAS – Ghid DCAF pentru parlamentarii vest-africani] (ECOWAS, 2011). Deține o diplomă de masterat în administrație publică din partea Universității Twente și o diplomă de doctorat în științe sociale din partea Universității Tilburg (Olanda).

AIDAN WILLS este coordonator de proiect în Departamentul de cercetare al DCAF, unde a lucrat vreme de șase ani pe tema guvernanței în domeniul intelligence și al securității. A fost principalul consultant la redactarea compilației Națiunilor Unite de bune practici privind serviciile de informații și supravegherea acestora. Mai recent, Aidan a fost coautor al unui studiu important al Parlamentului European, intitulat *Parliamentary Oversight of Security and Intelligence Services in the European Union* [Supravegherea parlamentară a serviciilor de securitate și de informații în Uniunea Europeană] și a fost coeditor al volumului *International Intelligence Cooperation and Accountability* [Cooperarea internațională în domeniul intelligence și responsabilitatea]. A predat cursuri de formare în cadrul unor organisme de supraveghere în domeniul intelligence și al securității din Europa și Orientul Mijlociu și a contribuit la diferite procese legislative. Aidan a lucrat în calitate de consultant la Consiliul

Europei, Parlamentul European și pentru Raportorul Special al Națiunilor Unite (pentru drepturile omului și combaterea terorismului) cu privire la diferite aspecte referitoare la guvernanța sectorului de securitate și drepturile omului. În prezent, este implicat în elaborarea, sub coordonarea Fundației pentru o Societate Deschisă, a unei compilații intitulate *Global Principles on National Security and the Right to Information* [Principii globale privind securitatea națională și dreptul la informație].

MONICA DEN BOER este angajată la Academia de Poliție din Olanda și este membră a Comisiei pentru Integrare Europeană din cadrul Consiliului Consultativ pentru Afaceri Internaționale. În 1990, a obținut o diplomă de doctorat din partea Institutului Universitar European și a lucrat la Universitatea din Edinburgh, la Centrul de Studii pentru Criminalitate și Aplicare a Legii din Olanda, la Institutul European de Administrație Publică, la Universitatea Tilburg și la Institutul European pentru Cooperare în Aplicarea Legii. Între martie 2004 și ianuarie 2012, a fost profesor de administrație publică comparată la Universitatea VU din Amsterdam, din partea Academiei de Poliție din Olanda. În 2009, a fost membră a Comisiei olandeze de Investigare pentru Irak, iar în 2009-2010 a participat la Grupul de Studiu privind Viitorul Apărării. A publicat numeroase lucrări despre cooperarea europeană în domeniul securității interne și este implicată în activități de predare, instruire și supervizare.

STUART FARSON este profesor auxiliar de științe politice la Universitatea Simon Fraser. În 1989-1990 a fost director de cercetare pentru prima și singura revizuire parlamentară statutară a Legii privind Serviciul Canadian pentru Informații de Securitate. A fost martor expert pentru Comisia de anchetă privind acțiunile oficialilor canadieni în cazul Maher Arar. Mai recent, a fost coautor, împreună cu Reg Whitaker, al lucrării *Accountability in and for National Security* [Responsabilitatea în și pentru securitatea națională], IRPP Choices (2009). A fost coeditor al lucrării *Commissions of Inquiry and National Security* [Comisiile de anchetă și securitatea națională] (2011) și al manualului intitulat *PSI Handbook of Global Security and Intelligence: National Approaches* [Manualul Praeger Security International privind securitatea globală și intelligence: abordări naționale] (2008), ambele publicate de Praeger.

CRAIG FORCESE este prodecan și profesor asociat la Facultatea de Drept (Secția Drept Comun), Universitatea din Ottawa. Predă drept public internațional, legislație în domeniul securităţii naţionale, drept administrativ și legislație publică. Mare parte din cercetările și scrierile sale actuale se referă la securitatea națională, drepturile omului și responsabilitatea democratică. În prezent, Craig este președintele Consiliului Canadian de Drept Internațional. Printre altele, el este autorul lucrării *National Security Law: Canadian Practice*

in International Perspective [Legislația privind securitatea națională: practica din Canada în perspectivă internațională] (Irwin Law, 2008) și coeditor al lucrării *Human Rights and Anti-terrorism* [Drepturile omului și combaterea terorismului] (Irwin Law, 2008).

GABRIEL GEISLER MESEVAGE este doctorand la Institutul de Înalte Studii Internaționale și de Dezvoltare unde lucrează și ca asistent cadru didactic. Totodată, a lucrat și ca asistent cercetător la acelaşi institut, studiind corupția în sectorul privat. Din 2010-2011, Gabriel a lucrat la DCAF, în Departamentul de cercetare, unde activitatea sa s-a axat pe guvernanța poliției și a serviciilor de informații. În această perioadă la DCAF, Gabriel a contribuit la secțiunea privind supravegherea externă din lucrarea DCAF *Toolkit on Police Integrity* [DCAF – Set de instrumente privind integritatea poliției]. Are o diplomă de masterat First Class Honours în relații internaționale și antropologie socială, acordată de Universitatea St Andrews și o diplomă de masterat în studii internaționale acordată de Institutul de Înalte Studii Internaționale și de Dezvoltare.

LAUREN HUTTON lucrează din 2005 ca cercetător și practician pe problematica reformării sectorului de securitate și a transformărilor post-conflict în Africa. În prezent, este consultant pentru Danish Demining Group (Grupul Danez pentru Deminare) și Danish Refugee Council (Consiliul Danez pentru Refugiați) în sudul Sudanului, ocupându-se în mod special de sensibilitatea la conflicte și reducerea violenței armate. Lauren a lucrat anterior pentru Saferworld și pentru Institutul pentru Studii de Securitate (ISS). În perioada în care a activat la ISS, Lauren a elaborat un proiect privind guvernanța democratică în domeniul intelligence în Africa. În acest mod, în 2007, a contribuit la procesele de verificare a activității de intelligence, iar, în 2009 și 2010, la elaborarea proiectelor de lege în domeniu, în Africa de Sud și a asigurat pregătirea parlamentarilor din sudul și estul Africii cu privire la supravegherea serviciilor de informații. De asemenea, în această perioadă a editat un volum despre intelligence și democrație în Africa de Sud, intitulat *To spy or not to spy* [A spiona sau a nu spiona] și a publicat mai multe articole de presă și lucrări ocazionale privind guvernanța în domeniul intelligence. Lauren are o diplomă de masterat în studii politice, acordată de Universitatea Western Cape (Africa de Sud).

IAN LEIGH este profesor de drept la Universitatea din Durham și membru al Institutului de Securitate Globală din Durham. Printre cărțile sale se numără *In From the Cold: National Security and Parliamentary Democracy* [Dezghețul: securitatea națională și democrația parlamentară] (Oxford University Press, 1994), cu Laurence Lustgarten, *Who's Watching the Spies: Establishing*

Intelligence Service Accountability [Cine supraveghează spionii: stabilirea responsabilității serviciului de informații] (Potomac Books, 2005), cu Hans Born și Loch Johnson, și *International Intelligence Cooperation and Accountability* [Cooperarea internațională în domeniul intelligence și responsabilitatea] (Routledge, 2011), cu Hans Born și Aidan Wills. Raportul său *Making Intelligence Accountable* [Responsabilizarea în domeniul intelligence] (cu Dr. Hans Born, publicat de Editura Parlamentului Norvegiei, 2005) a fost tradus în 14 limbi. Totodată, a fost co-autor al lucrării *OSCE/DCAF Handbook on Human Rights and Fundamental Freedoms of Armed Forces Personnel* [Manualul OSCE/DCAF privind drepturile omului și libertățile fundamentale ale personalului din forțele armate] (Varșovia 2008) și a activat în calitate de consultant la Biroul OSCE pentru Instituții Democratice și Drepturile Omului, la Comisia de la Veneția, pe teme referitoare la controlul democratic al agențiilor de securitate și informații în statele Consiliului Europei, și la PNUD, pe teme referitoare la reforma sectorului de securitate.

LAURIE NATHAN este profesor extraordinar și director al Centrului pentru Mediere din cadrul Universității din Pretoria. Este profesor invitat la Universitatea Cranfield, unde predă un curs de masterat despre reforma în domeniul intelligence. Cea mai recentă carte a sa se intitulează *Community of Insecurity: SADC's Struggle for Peace and Security in Southern Africa* [Comunitatea de insecuritate: lupta SADC pentru pace și securitate în Africa Australă], Ashgate (2012). A lucrat în Comisia ministerială de verificare a serviciilor de informaţii din Africa de Sud (2006-2008) și a redactat proiectul Cărţii Albe pentru Apărare a Africii de Sud (1996). A fost membru al următoarelor structuri: Comisia Consultativă a Departamentului Arme al Human Rigths Watch; Consiliul Internațional al Centrului Carter pentru Soluționarea Conflictelor; și Grupul consultativ de experți al Rețelei PNUD pentru Practica Guvernanței Democratice. Este inclus în UN Mediation Roster [Lista Națiunilor Unite de mediatori] și în UN Roster of SSR Experts [Lista Națiunilor Unite de experți în reforma sectorului de securitate].

KENT ROACH este profesor de drept la Universitatea din Toronto, unde este titularul Catedrei de drept și politică publică Prichard Wilson. A fost membru al comitetului consultativ de cercetare al Comisiei de anchetă privind acțiunile oficialilor canadieni în cazul Maher Arar și director de cercetare al Comisiei de anchetă pentru investigarea exploziei cu bombă din cursa 182 a companiei Air India. Cea mai recentă carte a sa este *The 9/11 Effect: Comparative Counter-Terrorism* [Efectul 11 septembrie: abordare comparativă a luptei împotriva terorismului], publicată de Cambridge, în 2011.

BERT VAN DELDEN s-a alăturat puterii judecătorești din Olanda în 1966. A fost președinte al Tribunalului Districtual din Haga în perioada 1990-2001 și a fost numit apoi prim președinte al Consiliului pentru Puterea Judecătorească. După retragerea sa din activitatea judiciară, a fost numit membru al Comisiei olandeze de Verificare a Serviciilor de Informații și de Securitate (CTIVD). Din 2009, a fost președintele acestei comisii.

THEODOR H. WINKLER este directorul Centrului pentru Controlul Democratic al Forțelor Armate din anul 2000, atunci când Consiliul Federal elvețian l-a promovat la rangul de ambasador și l-a numit șef al centrului nou înființat. S-a alăturat Departamentului elvețian al Apărării la sfârșitul anului 1981, în calitate de expert pe probleme de securitate internațională. În 1985 a fost numit reprezentant al șefului de stat major pe probleme politico-militare, iar în 1995 a devenit șeful Departamentului nou creat pentru politica de securitate internațională. Ulterior a fost promovat la rangul de șef adjunct pentru politica de securitate și apărare. Winkler a studiat științe politice și securitate internațională la Universitatea din Geneva, la Universitatea Harvard și la Institutul de Înalte Studii Internaționale din Geneva. În 1981 a obținut o diplomă de doctorat în științe politice cu o teză despre proliferarea nucleară.



Supravegherea serviciilor de informații

Set de instrumente

Acest set de instrumente este un compendiu de lucrări scrise de cei mai importanți experți în guvernanța domeniului intelligence din întreaga lume. El oferă orientări relevante pentru politicile referitoare la înființarea și consolidarea sistemelor de supraveghere a serviciilor de informații, precum și la supravegherea unor componente specifice din activitatea serviciilor de informații, ce cuprind: culegerea de informații, utilizarea datelor cu caracter personal, schimbul de informații cu parteneri din țară şi din străinătate, precum și finanțele serviciilor. Ghidul se bazează pe diverse tipuri de legislații și structuri instituționale și pe practica din numeroase state.

Cu toate că acest set de instrumente analizează cu precădere organismele de supraveghere parlamentare și independente, el conține numeroase analize care sunt relevante pentru puterea executivă, cea judecătorească, mass-media, societatea civilă și chiar pentru serviciile de informații. Această lucrare va prezenta, probabil, un deosebit interes pentru membrii și personalul organismelor de supraveghere, pentru actori implicați în monitorizarea activității celor care efectuează supravegherea (de exemplu, mass-media, organizații ale societății civile și parlamentari) și pentru subiecții supravegherii externe: executivul și serviciile de informații.

Centrul pentru controlul democratic al forțelor armate (DCAF) de la Geneva este o fundație internațională cu misiunea de a sprijini comunitatea internațională în realizarea bunei guvernanțe și reformarea sectorului de securitate. Centrul dezvoltă și promovează norme și standarde, realizează cercetări tematice individualizate, identifică bune practici și recomandări pentru promovarea guvernanței democratice în sectorul de securitate și asigură sprijin consultativ la nivel de țară, precum și programe de asistență cu caracter practic.

www.dcaf.ch